Behaviour Profiling for Mobile Devices

by

Fudong Li

A thesis submitted to the Plymouth University in partial fulfilment for the degree of

DOCTOR OF PHILOSOPHY

February 2012

Copyright Statement

Abstract

Behaviour Profiling for Mobile Devices

Fudong Li

With more than 5 billion users globally, mobile devices have become ubiquitous in our daily life. The modern mobile handheld device is capable of providing many multimedia services through a wide range of applications over multiple networks as well as on the handheld device itself. These services are predominantly driven by data, which is increasingly associated with sensitive information. Such a trend raises the security requirement for reliable and robust verification techniques of users.

This thesis explores the end-user verification requirements of mobile devices and proposes a novel Behaviour Profiling security framework for mobile devices. The research starts with a critical review of existing mobile technologies, security threats and mechanisms, and highlights a broad range of weaknesses. Therefore, attention is given to biometric verification techniques which have the ability to offer better security. Despite a large number of biometric works carried out in the area of transparent authentication systems (TAS) and Intrusion Detection Systems (IDS), each have a set of weaknesses that fail to provide a comprehensive solution. They are either reliant upon a specific behaviour to enable the system to function or only capable of providing security for network based services. To this end, the behaviour profiling technique is identified as a potential candidate to provide high level security from both authentication and IDS aspects, operating in a continuous and transparent manner within the mobile host environment.

This research examines the feasibility of a behaviour profiling technique through mobile users general applications usage, telephone, text message and multi-instance application usage with the best experimental results Equal Error Rates (EER) of 13.5%, 5.4%, 2.2% and 10% respectively. Based upon this information, a novel architecture of Behaviour Profiling on mobile devices is proposed. The framework is able to provide a robust, continuous and non-intrusive verification mechanism in standalone, TAS or IDS modes, regardless of device hardware configuration. The framework is able to utilise user behaviour to continuously evaluate the system security status of the device. With a high system security level, users are granted with instant access to sensitive services and data, while with lower system security levels, users are required to reassure their identity before accessing sensitive services.

The core functions of the novel framework are validated through the implementation of a simulation system. A series of security scenarios are designed to demonstrate the effectiveness of the novel framework to verify legitimate and imposter activities. By employing the smoothing function of three applications, verification time of 3 minutes and a time period of 60 minutes of the degradation function, the Behaviour Profiling framework achieved the best performance with False Rejection Rate (FRR) rates of 7.57%, 77% and 11.24% for the normal, protected and overall applications respectively and with False Acceptance Rate (FAR) rates of 3.42%, 15.29% and 4.09% for their counterparts.

Contents

List of Figures vii
List of Tables x
Acknowledgement xiii
Author's Declaration xiv
1 Introduction & Overview 15
1.1 Introduction 15
1.2 Aims and objectives 17
1.3 Thesis structure 18
2 The evolution of Mobile Devices 20
2.1 Introduction 20
2.2 Mobile communication technologies and mobile devices 20
2.2.1 Mobile cellular technologies 20
2.2.2 Other mobile communication technologies 23
2.2.3 Mobile devices 25
2.3 Mobile device security threats 29
2.3.1 Mobile service fraud 30
2.3.2 Denial of Service attack 30
2.3.3 Mobile malware 31
2.3.4 Social engineering attack 33
2.3.5 Loss or theft of the device 33
2.4 Mobile security controls 34
2.4.1 Authentication 35
2.4.2 Mobile Antivirus solutions 36
2.4.3 Mobile Firewall products 36
2.4.4 Mobile Encryption 37
2.4.5 Battery monitoring based mobile IDS 37
2.5 Conclusion 39
3 Review of Biometric Authentication 41
3.1 Introduction 41
3.2 An introduction of the biometric system 41
3.2.1 A generic biometric system 42

3.2.2 Biometric system performance measurement factors 45
3.2.3 Biometric system requirement 47
3.3 Biometric characteristics 47
3.3.1 Physiological biometrics 48
3.3.2 Behavioural biometrics 56
3.4 Biometric approaches applicable for use on a mobile device 64
3.5 Literature review on behaviour profiling 68
3.5.1 Telephony service based mobile IDS 68
3.5.2 Migration based mobile IDS 70
3.5.3 Comparison of behaviour based mobile IDS 73
3.6 Conclusion 73
4 Behavioural Profiling on Mobile Devices 75
4.1 Introduction 75
4.2 Methodology 76
4.2.1 Dataset 76
4.2.2 Procedure 79
4.3 The results 81
4.3.1 A Descriptive statistics study 81
4.3.2 A preliminary study on telephony activity 97
4.3.3 Behaviour profiling on mobile applications 103
4.4 Discussion 112
4.5 Conclusion 114
5 A Novel Framework for Behaviour Profiling on Mobile Devices 116
5.1 Introduction 116
5.2 A Novel Behaviour Profiling Framework 116
5.3 Processing Engines 117
5.3.1 Data Collection Engine 118
5.3.2 Behaviour Profile Engine 121
5.3.3 Behaviour Classification Engine 126
5.3.4 Communication Engine 129
5.4 Security Status Module 131
5.5 Inventory database 134
5.6 Security Manager 136

5.6.1 Standalone mode 136
5.6.2 Dependent mode 139
5.7 Conclusion 141
6 Evaluation of the Behaviour Profiling Framework 143
6.1 Introduction 143
6.2 Simulation Implementation 143
6.3 Simulation process 145
6.3.1 Simulation results – Scenario A 146
6.3.2 Simulation results – Scenario B 147
6.3.3 Simulation results – Scenario C 148
6.3.4 Simulation results – Scenario D 150
6.4 Discussion 152
6.5 Conclusion 154
7 Conclusions and Future Work 155
7.1 Achievements of the research 155
7.2 Limitations of the research project 157
7.3 Suggestions & Scope for Future Work 158
7.4 The Future of Verification for Mobile Devices 159
References 160
Appendix A: The MIT Reality dataset 175
Appendix B: The Neural Networks and the rule-based classifiers scripts 175
Appendix C: The simulation scripts 175
Appendix D: The preliminary study's experimental results 175
Appendix E: The final experimental results 175
Appendix F: Publications 175
- Misuse Detection for Mobile Devices Using Behaviour Profiling 175
- Behaviour Profiling for Transparent Authentication for Mobile Devices 175
- Behaviour Profiling on Mobile Devices 175
- Intrusion Detection System for Mobile Devices: Investigation on Calling Activity 175

List of Figures

Figure 2.1: 3G: Cumulative network launches worldwide 22
Figure 2.2: Wi-Fi market projections 2005-2012 23
Figure 2.3: Mobile communication technologies data rate vs. mobility 25
Figure 2.4: Consumer mobile platform activities 2011 29
Figure 2.5: The distribution of malware by platform 32
Figure 2.6: An example of Android password pattern 36
Figure 3.1: A generic biometric system 42
Figure 3.2: A biometric verification process 44
Figure 3.3: A biometric identification process 45
Figure 3.4: Mutually Exclusive Relationship between FAR/FRR 46
Figure 3.5: An anatomical sketch of a human ear 49
Figure 3.6: An example of face recognition 50
Figure 3.7: An example of human face thermo image 51
Figure 3.8: An example of Fingerprint Recognition 52
Figure 3.9: An example of hand geometry scanner 54
Figure 3.10: An example of a human eye 55
Figure 3.11: An example of palm scanner 56
Figure 3.12: BlackBerry and iPhone average Application Usage comparison 57
Figure 3.13: Gait cycle 58
Figure 3.14: An example of a handwritten signature on a computing device 59
Figure 3.15: An example of keystroke analysis 60
Figure 3.16: Biometric Revenues by Technology 63
Figure 3.17: Biometric Industry Revenues 63
Figure 3.18: Biometric approaches on a mobile device 64
Figure 3.19: A generic TAS framework 67
Figure 4.1: Behaviour profiling system functions flow diagram 80
Figure 4.2: The three classifiers being employed 80
Figure 4.3: Users with their applications 82
Figure 4.4: Overview of intra-standard application usage 83
Figure 4.5: The location comparison for all users' camera application usage 84
Figure 4.6: The location comparison for all users' logs application usage 85
Figure 4.7: The location comparison for all users' message centre application usage 86

Figure 4.8: The location comparison for all users' phonebook application usage 87
Figure 4.9: The time of accessing comparison for users' camera application usage 88
Figure 4.10: The time of accessing comparison for users' logs application usage 88
Figure 4.11: The time of accessing comparison for users' message centre application usage 89
Figure 4.12: The time of accessing comparison for users' phonebook application usage 89
Figure 4.13: Users telephony location usage comparison 90
Figure 4.14: Users telephony telephone number usage comparison 91
Figure 4.15: Users telephony time of calling comparison 92
Figure 4.16: Users telephony duration of calling comparison 93
Figure 4.17: A cumulative distribution for all users' telephone call duration 93
Figure 4.18: Location usage comparison of users' text message 94
Figure 4.19: Users text message telephone number usage comparison 95
Figure 4.20: Users text message time of sending comparison 96
Figure 4.21: FAR-FRR plot for the RBF network performance (Inputs: telephone number and location with 75 neurons) 98
Figure 4.22: FAR-FRR plot for the FF MLP network performance (Inputs: telephone number and location with 150 neurons) 99
Figure 4.23: FAR-FRR plot for the performance of the rule-based approach 101
Figure 4.24: FAR-FRR plot for intra-standard applications with the dynamic 14 day profile with 1 application entry 104
Figure 4.25: FAR-FRR plot for intra-standard applications with the dynamic 14 day profile with 6 application entries 105
Figure 4.26: FAR-FRR plot for the telephone call application with the dynamic 14 day profile with 1 telephone call entry 106
Figure 4.27: FAR-FRR plot for the telephone call application with the dynamic 14 day profile with 6 telephone call entries 107
Figure 4.28: FAR-FRR plot for the text messaging application with the dynamic 14 day profile with 1 text message entry 108
Figure 4.29: FAR-FRR plot for the text messaging application with the dynamic 14 day profile with 3 text message entries 109
Figure 4.30: FAR-FRR plot for multi-instance applications with the dynamic 10 day profile with 1 application entry 111

Figure 4.31: FAR-FRR plot for multi-instance applications with the dynamic 10 day profile with 6 application entries 111
Figure 5.1: A novel Behaviour Profiling Framework 117
Figure 5.2: Data Collection Engine 118
Figure 5.3: Behaviour Profile Engine 122
Figure 5.4: Behaviour Classification Engine 127
Figure 5.5: the verification requirement checking processes of the Behaviour Profiling Engine 128
Figure 5.6: Communication Engine 130
Figure 5.7: The SS level calculation process 133
Figure 5.8: The SS level degradation function 133
Figure 5.9: Security Manager: Process Algorithm 137
Figure 5.10: TAS two tier authentication approach 140
Figure 5.11: The Android HIDS architecture 141

List of Tables

Table 2.1: The evolution of cellular mobile communication technologies 21
Table 2.2: 3G services with their QoS requirements 22
Table 2.3: Mobile device (2010) VS PC (2001) 26
Table 2.4: Examples of App stores in 2011 26
Table 2.5: Applications with their risk scores 27
Table 2.6: Examples of mobile services 28
Table 2.7: Example of Mobile malware and its effects 32
Table 2.8: A summary of battery based mobile IDS 38
Table 2.9: Mobile security mechanisms vs. Mobile security threats 39
Table 3.1: A brief comparison on biometrics approaches 62
Table 3.2: Biometric approaches on mobile devices 68
Table 3.3: A review of mobile behaviour profiling 73
Table 4.1: The MIT Reality dataset 77
Table 4.2: The final dataset on intra-standard applications 78
Table 4.3: The final dataset on telephony service 78
Table 4.4: The final dataset on text messaging service 79
Table 4.5: The cell comparison for User 22 and User 40's camera application usage 84
Table 4.6: The cell comparison for User 43 and User 50's logs application usage 85
Table 4.7: The cell comparison for User 59 and User 73's message centre application usage 86
Table 4.8: The Cell comparison for User 41 and User 66's phonebook application usage 87
Table 4.9: Telephony location usage comparison for user 20 and user 36 90
Table 4.10: Telephone number usage comparison for user 20 and user 36 91
Table 4.11: The location usage comparison for user 3's and user 12's text messaging service 94
Table 4.12: Text message telephone number usage comparison for user 6 and user 12 95
Table 4.13: The best RBF network configurations with various features 98
Table 4.14: The best FF MLP network configurations with various features 99
Table 4.15: Experimental results by employing the rule-based approach 100
Table 4.16: Individual application features towards to the classification result 101
Table 4.17: Experimental results for intra-standard applications 104
Table 4.18: Selected users' performance for intra-standard applications, employing the best classifier configurations 105

Table 4.19: Experimental results for the telephone call application 106
Table 4.20: Selected users' performance for the telephone call application by employing the best classifier configuration 107
Table 4.21: Experimental results for the text messaging application 108
Table 4.22: Selected users' performance for the text messaging application with the dynamic 14 day profile and 3 log entries 109
Table 4.23: Experimental results for multi-instance applications 110
Table 4.24: Selected users' performance for multi-instance applications with the dynamic 10 day profile and 6 log entries 112
Table 4.25: The behavioural techniques performance within the mobile device environment 114
Table 5.1: Applications record 118
Table 5.2: Temporary Storage 120
Table 5.3: Application Features Record 121
Table 5.4: Behavioural Input Data 121
Table 5.5: Application Category 121
Table 5.6: Application name 121
Table 5.7: Application Features 121
Table 5.8: Behaviour Template 123
Table 5.9: Behaviour Audit Log 124
Table 5.10: Smoothing Function 125
Table 5.11: Application Performance Factor 132
Table 5.12: System Security levels 134
Table 5.13: User's information 135
Table 5.14: Three main checking stages 136
Table 6.1: Four scenarios for the simulation process 146
Table 6.2: Simulation results of scenario A for legitimate users 147
Table 6.3: Simulation results of scenario A for imposters 147
Table 6.4: Simulation results of scenario B for legitimate users 148
Table 6.5: Simulation results of scenario B for imposters 148
Table 6.6: Simulation results of scenario C for legitimate users 149
Table 6.7: Simulation results of scenario C for imposters 149
Table 6.8: Simulation results of scenario D for legitimate users 150
Table 6.9: Simulation results of scenario D for imposters 151

Table 6.10: The statistic on the smoothing function usage for all four scenarios 151
Table 6.11: The statistic on the usage of the “check if there are any applications not being processed before the protected application” clause 152

Acknowledgement

The research project was made possible due to the full scholarship funding provided by Plymouth University and the pleasant facility offered by the Centre for Security, Communication and Network Research (CSCAN), Plymouth University, UK. I wish to thank both organisations for their support.

This PhD work would not have been possible without the guidance and help of my Director of Studies, Associate Professor Nathan L Clarke. Thanks go to him for his tireless support and inspiring advice throughout the PhD process, from conducting experiments to publishing research papers.

Thanks must also go to my other supervisors, Dr Maria Papadaki and Associate Professor Paul Dowland, who provided invaluable help and guidance throughout my PhD journey, and spent significant amount of time for proof reading research papers and my thesis.

Thanks also go to my fellow researchers within the CSCAN group (especially Mr Christopher Hocking) for their support and interesting discussions.

Finally, I would like to thank my parents who spiritually and financially supported me for my student life. Also, I wish to thank my beloved wife for her endless care, support and encouragement.

Author's Declaration

At no time during the registration for the degree of Doctor of Philosophy has the author been registered for any other University award without prior agreement of the Graduate Committee.

This study was financed with the aid of scholarship from Faculty of Science and Technology, Plymouth University, Plymouth, United Kingdom.

Relevant seminars and conferences were regularly attended at which work was often presented and several papers were published in the course of this research project.

Word count of main body of thesis: 45,701 words

Signed……

Date……

1 Introduction & Overview

1.1 Introduction

Whilst the term mobile devices can refer to a variety of devices, such as mobile phones, laptops and games consoles, the mobile phone and its variants form the largest market segment. In this thesis, the phrase 'mobile device' describes two kinds of mobile computing devices: the standard mobile phone and the Smartphone. After almost 40 years of development, the mobile device has transformed from a purely telephony based handset into a multimedia and multi-networking computing device. Currently, with more than 5 billion subscribers around the world, the mobile device has become a ubiquitous object within our daily life (GSM World, 2011). People can utilise it to complete various tasks, such as making telephone calls, surfing the Internet, checking emails, transferring money, playing games, viewing documents and storing information; to name but a mere fraction of the functionality and applications available.

In order to accommodate these services, the mobile device has become incredibly powerful in terms of processing power, networking ability and data storage. Some mobile device Central Processing Units (CPU) clock up to 1.5 GHz allowing many complex programs (e.g. high definition games) to be run smoothly on them (Qualcomm, 2010). With the availability of various wireless technologies such as Wi-Fi and NFC (Near Field Communication), people can utilise many network-based services in additional to telephony and text messaging. For instance, by using a Wi-Fi network, a mobile device user can access web pages, check emails and shop online. At the start of 2011, over 50% of mobile users (more than 2.5 billion) connected to the Internet via a Wi-Fi connection (Cabume, 2011). Moreover, in 2011 the total number of mobile devices connecting with Wi-Fi networks overtook the number of laptops accessing the same resource (GigaOM, 2011). As the JiWire Mobile Audience Insights Report suggested, 47% of all mobile device users use the Internet as their primary source for online shopping in the US (JiWire, 2009). According to a survey conducted by the Internet Advertising Bureau (IAB), over 23 million people use their mobile devices to make online purchases in the UK (Newbusiness, 2010). The latest BRC-Google retail monitor found that mobile online shopping increased by 27% in the second quarter of 2011 (Walesonline, 2011). Another example is that the mobile device can be transformed into a mobile wallet that enables people to pay for goods directly from their handset by connecting with a NFC payment device. In the UK, the mobile operator Orange launched the first mobile payment service which allows their customers to buy food in superstores imitating a service that has been used in

Japan and Korea for many years (BBC, 2011). According to the Juniper Research, mobile payment via NFC will generate $50 billion of revenue by 2014 around the world (Knowyourmobile, 2011).

Being equipped with internal memory and other an external micro Secure Digital (SD) card, the storage capability of the mobile device has increased significantly. Today, a typical mobile device has a data capacity of up to 32 GigaBytes (GB) enabling a large amount of information, such as text messages, calendar entries, pictures, Word documents, to-do lists and emails, to be stored. A number of studies have demonstrated that such information is highly likely to be related to personal, financial or business data. Which? Mobile (2011) showed that 13.5 million UK mobile users stored personal information (e.g. date of birth) on the device. Also, Regenersis' study revealed that 99% of 2,000 randomly selected mobile devices contained some amount of personal data (Regenersis, 2009). Moreover, the Smartphone IT security survey of Kaspersky Lab showed that approximately 33% of the 1,600 surveyed stored login credentials (i.e. user name and password) for accessing personal and business email accounts on their mobile devices (Kaspersky Lab, 2011a). The mobile and security report of McAfee also indicated that more than 20% of organisations' employees store business critical data, such as customer data, corporate intellectual property or financial information on their mobile device (McAfee, 2011b).

While people enjoy the convenience provided by the mobile device, the services and the information stored on the device pose an increasing threat to the owners when a device is misused, such as being lost or stolen or infected by malware. According to the Metropolitan Police (2011) website there are more than 10,000 mobile devices lost or stolen in London every month. Traditionally, the cost of the hardware was the driving factor for theft. However, the increased functionality and access to information could drive the prime motivation towards information theft. By using the services and information, malicious users can abuse the mobile devices in many ways. For instance, buy goods in a shop or online at the owner's expense, review the personal information and eventually steal the owner's identity (Helium, 2008). If a stolen device belongs to a company, malicious users could sell the information stored on the device to its competitors; also, by using the device as a gateway, malicious users could harvest more information from the company internal network. Since the first mobile virus 'Cabir' was reported in 2004 (BBC, 2004), over 1,000 unique variants were already identified by the end of 2010 (Kaspersky Lab, 2011b). These malware attack mobile devices regardless of platform and may cause severe damage, such as disabling mobile services, sending text messages to a premium rate service or stealing data (Securelist, 2009). Therefore, it is mission critical to protect the mobile device from being misused.

Currently, the most popular mobile device access control is the password or Personal Identification Number (PIN) based authentication approach. This technique requires users to provide a correct PIN before gaining access to the mobile device regardless of their legitimacy. Although this approach is mostly available on mobile devices, a survey conducted by Credant demonstrated that alarmingly 40% of their participants failed to utilise this simple point-of-entry security mechanism (Credant, 2009). Even if all mobile users employed this technique on their devices possible misuse could still occur if they did not use it properly in practice, such as never changing the PIN, writing the PIN on a paper or sharing the PIN with others (Clarke and Furnell, 2005; Kurkovsky and Syta, 2010). To protect the mobile device against malware attacks a number of mobile antivirus and firewall software are already commercially available. However, as they are heavily reliant upon the latest signatures to detect malware presence they are not effective against zero day attacks. Besides, their ability to detect user related misuse such as viewing calendar events or modifying documents is limited. To date, only behaviour based network Intrusion Detection Systems (IDS) are capable of detecting mobile users' abnormal activities (i.e. telephony service fraud) (Samfat and Molva, 1997; Gosset, 1998; Sun *et al*, 2006). This has not been a big issue as the mobile device could only access service providers' networks and offer telephony and text messaging services. However, as the modern mobile device can now access multiple networks and provides a wide range of host based services a more sophisticated method which can provide continuous protection for all the mobile services is needed.

1.2 Aims and objectives

The aim of this research is to propose a behavioural profiling security framework for mobile devices which is capable of fulfilling the increased security requirements and providing continuous protection to ensure the legitimacy of the current user. Also, the framework would work in three distinct modes: a standalone security control (standalone mode), a transparent authentication mechanism (Transparent Authentication System (TAS) mode) and a misuse detector (IDS mode).

The main objective for this research is to explore, propose and evaluate a behavioural profiling approach which enhances the security for the mobile device. In order to achieve this, this project is divided into five distinct stages:

1. To investigate the security requirements for the mobile device and identify the need for a behavioural profiling security approach.

2. To compose a comprehensive review of biometric authentication approaches and examine the applicability of deploying a behaviour profiling technique on mobile devices.
3. To design a series of experiments for exploring the feasibility of deploying a behaviour profiling approach on mobile devices.
4. To propose a novel security framework to support the aim of behaviour profiling on mobile devices in a continuous and transparent manner.
5. To evaluate the security effectiveness of the proposed behaviour profiling framework for mobile devices through a simulation method.

1.3 Thesis structure

Chapter 2 begins by reviewing mobile communication technologies along with current mobile services establishing the importance of the security of the mobile device. By presenting both potential security threats and existing security approaches, a need for a new security mechanism which can provide continuous and transparent protection for the mobile device is identified. The chapter concludes by highlighting the need for a more comprehensive and sophisticated security control and suggesting possible solutions.

Having established the need for a new security technique for mobile devices, Chapter 3 presents and discusses the feasibility of utilising biometric verification techniques as a solution for tackling this issue. Chapter 3 starts by presenting a generic biometric model and biometric system performance measurement and requirement factors. The chapter then proceeds to describe an overview of existing biometric techniques based upon their physiological or behavioural characteristics. By comparing all applicable biometric approaches for the mobile device, a novel behaviour profiling based technique was chosen due to its various advantages. The chapter concludes by undertaking a comprehensive literature review on mobile behaviour profiling techniques to date.

Chapter 4 introduces a number of experimental studies into the feasibility of behaviour profiling on a mobile device. The studies have been based upon examining user interactions with mobile devices to verify the user, especially, the way in which users utilise intra-standard and intra-extended applications. By comparing a number of pattern classification methods based upon statistical and artificial intelligence algorithms in a preliminary study, a number of application features towards success verification and the most appropriate classifier have been identified. The chapter finishes with evaluating the behaviour profiling technique on mobile user application

usage via the combination of the rule based approach, a dynamic profiling technique and a smoothing function.

Chapter 5 presents a novel Behaviour Profiling framework which provides transparent and continuous protection for mobile devices to fulfil two security purposes: authentication and IDS. The framework verifies the identity of a user based upon their applications usage. In order to provide more accurate verifications, a dynamic profiling technique which updates the profile of a user on a daily basis was utilised. Also, the framework reduces the impact of the high false rejection problem which every single behavioural biometric technique experiences by employing a smoothing function. The framework performs verification processes based upon three criteria (the smoothing function, a verification time and the sensitivity of an application) and updates a System Security (SS) level accordingly. The SS level introduces a level of intelligence to the framework: the identity of a user is not verified based upon a single pass or fail but a number of consecutive verification results. The chapter concludes by presenting a process algorithm which permits the behaviour profiling framework providing continuous and transparent security for mobile devices.

Chapter 6 evaluates the proposed the framework via a simulation. The chapter begins by describing the implementation of the simulation. The chapter finishes by presenting and discussing a number of scenarios that have been designed to examine various configurations of the Behaviour Profiling framework.

Finally, Chapter 7 presents the main conclusions from the research, highlighting its achievements and limitations. Future research and development for this project are also suggested in this chapter.

2 The evolution of Mobile Devices

2.1 Introduction

The mobile device was initially designed to provide a telephony service via a cellular network. With the widespread availability of newer wireless technologies and the evolution of the mobile device itself, they can now also utilise other network mechanisms, namely: Wi-Fi, Bluetooth and NFC. This firm foundation allows the mobile device to offer a wide range of network based services. For example, Internet surfing via Wi-Fi hotspots, video conferencing through a 3G connection, road navigating by a Global Positioning System (GPS) link, picture sharing by using Bluetooth pairing and data synchronisation with laptop/desktop computers via a Universal Serial Bus (USB) cable. People can utilise these services to carry out a huge variety of personal and business tasks.

2.2 Mobile communication technologies and mobile devices

2.2.1 Mobile cellular technologies

In 1979, the first fully automatic cellular network (the First Generation (1G) network) was launched in Japan. By using a Frequency Division Multiple Access (FDMA) multiplexing method over an analogue circuit, people were able to talk with each other over the air via their handsets for the first time. However, it was only the rich who had the luxury to experience the mobile telephony service. By providing a more reliable service and charging an affordable price to the general public, the Second Generation (2G) cellular networks gradually replaced the 1G cellular networks in the early 1990s. By employing digital circuit switching technology, the 2G cellular networks supported both voice and data services. The data service was offered in the form of the Short Messaging Service (SMS) which allowed mobile users to communicate with each other by short text messages.

Since the introduction of the SMS, a trend of providing higher data rate and more number of services started to emerge. Table 2.1 illustrates the evolution of mobile cellular services over the last 30 years. By deploying the Wireless Application Protocol (WAP) on the Second Generation Enhanced mobile network (2.5G), mobile users were able to access Internet based services (e.g. web surfing) at a data rate of 9.6 kilobit per second (kbps) around the year 2000.

	1G	2G	2.5G			3G	4G
Technical							
Standards			HSCSD	GPRS	EDGE	IM-2000	
Transmission type	Analogue	Digital	Digital	Digital	Digital	Digital	Digital
Data rate (per second)	-	9.6K	57.6K	114K	384K	2M	1G
Switching	Circuit	Circuit	Circuit	Packet	Circuit/ Packet	Packet	Packet
Multiplexing	FDMA	TDMA/ CDMA	TDMA	TDMA/ FDMA	TDMA/ FDMA		
Services							
Voice call	✓	✓	✓	✓	✓	✓	✓
SMS		✓	✓	✓	✓	✓	✓
Internet				✓	✓	✓	✓
MMS						✓	✓
Video call						✓	✓
Video conference						✓	✓
Watch TV program							✓
Miscellaneous							
Availability	1983	1992	2000	2001	2002	2001	2015

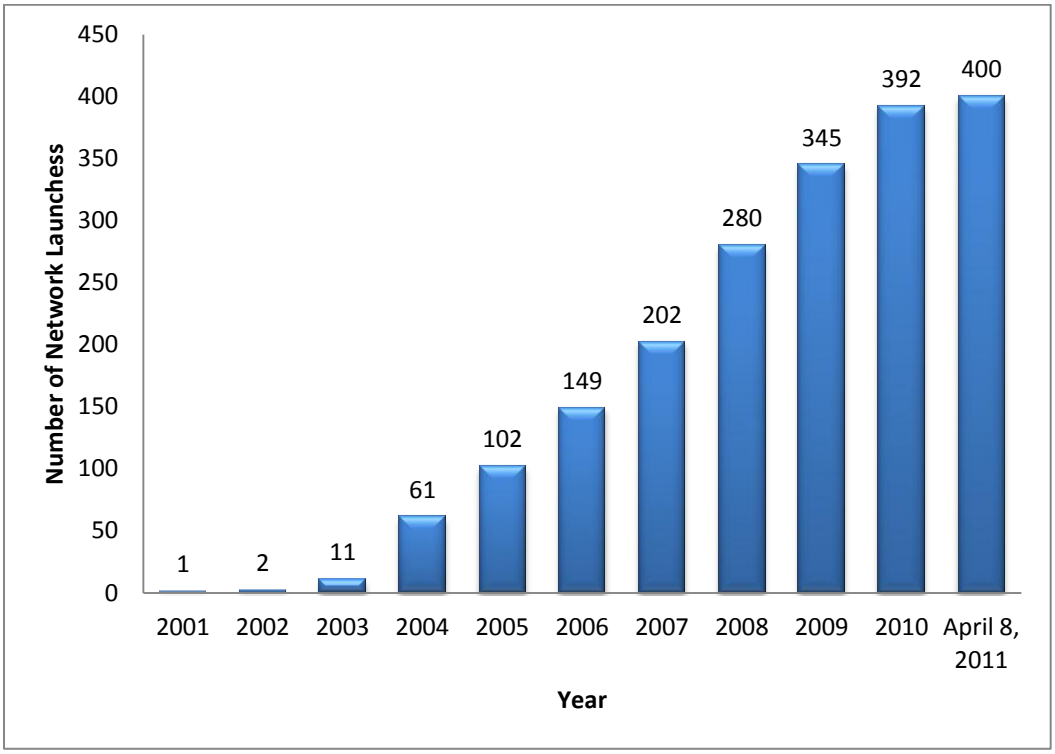
Adapted from: Clarke, 2004

Table 2.1: The evolution of cellular mobile communication technologies

Despite 2G network technology being first introduced nearly 20 years ago, it still dominates the current cellular communication market. By providing the service to more than 3.5 billion subscribers globally, 2G networks held almost an 80% share of the mobile communication market in 2009 (GSM World, 2009). Nonetheless, due to the rapid development of newer communication technologies, the revenue of 2G network has slowly declined over the last few years (Communications Today, 2010).

Since the first commercial Third Generation (3G) mobile network was launched by NTT DoCoMo in Japan in 2001, 3G technology has gradually been adopted. As shown in Figure 2.1, by the end of April 2011, a total of 400 3G networks had been successfully deployed around the world. With a maximum data rate of 2 Megabits per second (Mbps), 3G networks support many data services which were not previously available to mobile users, such as video conferencing and the Multimedia Messaging Service (MMS). Table 2.2 illustrates a number of available 3G services. Based upon their Quality of Service (QoS) requirements, a higher priority will be given to conversational services (i.e. voice calling and video conferencing) when they access a 3G network. In contrast, a lower network access priority will be applied to background services, such as email and SMS. With currently more than 650 million subscribers in the world, the 3G network holds

approximately 10% of the mobile communication market share (GSA, 2011b). Moreover, the future 3G market has been strongly predicted. For Europe alone, the number of 3G subscriptions will outnumber 2G in 2012. Also, in the same year, it is anticipated that approximately 70% of the total cellular subscriptions will be 3G network based (GSA, 2011a).



Source: GSA,2011b

Figure 2.1: 3G: Cumulative network launches worldwide

QoS Classes	Example of 3G services
Conversational	Voice, video telephony, video gaming
Streaming	Multimedia, video on demand, webcast
Interactive	Web browsing, network gaming, database access
Background	Email, SMS, downloading

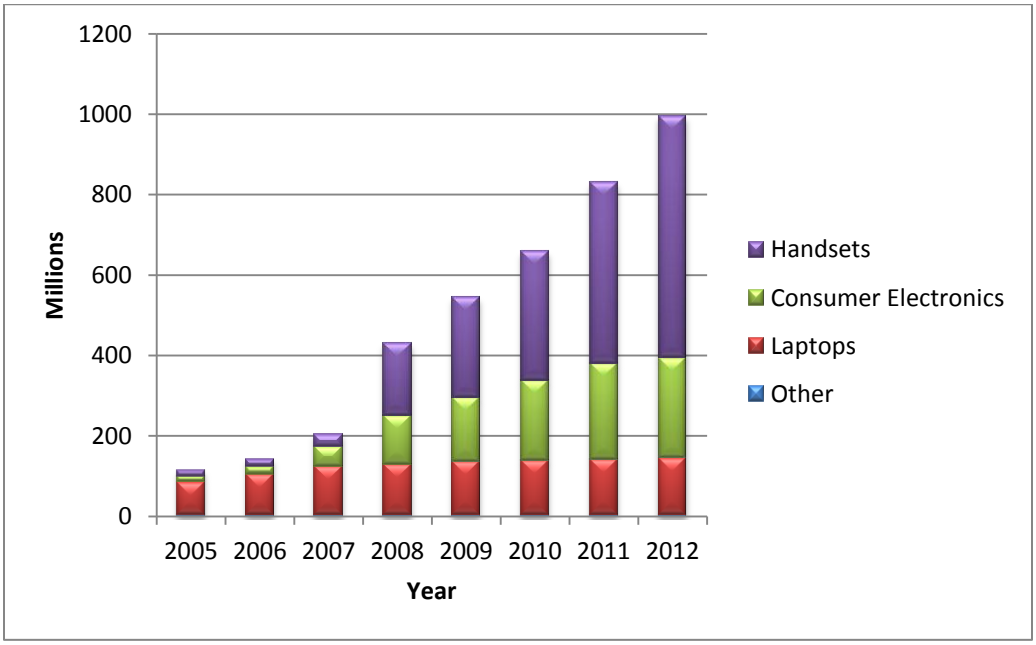
Table 2.2: 3G services with their QoS requirements

Other cellular technology, such as 3rd Generation Partnership Project Long Term Evolution (3GPP LTE), is also at the frontier of the mobile communication market. As its bandwidth does not meet the requirement of the Fourth Generation (4G) but is higher than the counterpart of the 3G, people refer to it as a pre-4G technology despite it being branded as a 4G technology in the market. Since its first appearance in 2009, LTE has experienced a steady growth in market share. In addition, the revenue of LTE technology is forecasted to be US$942 million in the US and a further $650 million from Western Europe in 2015 (PC advisor, 2010).

2.2.2 Other mobile communication technologies

Apart from accessing the aforementioned cellular communication technologies, mobile devices can also connect with a number of other communication technologies, namely Wi-Fi, Bluetooth, NFC, ZigBee and USB.

Wi-Fi is a general term for the IEEE 802.11 wireless technology standards. Wi-Fi technology enables computing devices to connect to the Internet, with a bandwidth up to 150 Mbps per stream, within an approximate range of up to 250 metres. By using a Wi-Fi connection, a mobile user can access many Internet based services, such as sending/receiving emails, chatting online and accessing web pages. Currently many network operators provide the Wi-Fi service around the world. BT alone offers 2.8 million Wi-Fi connections in the UK and Republic of Ireland (BTopenzone, 2011). This provides an additional platform via which mobile devices can be permanently connected. Although the coverage of a single Wi-Fi network is somewhat limited, by connecting a number of them together, a wireless mesh network can be formed which improves a user's mobility greatly. For example in London, a city-sized Wi-Fi network allows millions of mobile devices to be connected with high speed (BBC news, 2007). Figure 2.2 illustrates the Wi-Fi market projections between 2005 and 2012. It demonstrates that approximately 1 billion Wi-Fi enabled devices will be shipped in the year 2012. In addition, more than half of such devices will be mobile devices.



Source: Skyhook, 2007

Figure 2.2: Wi-Fi market projections 2005-2012

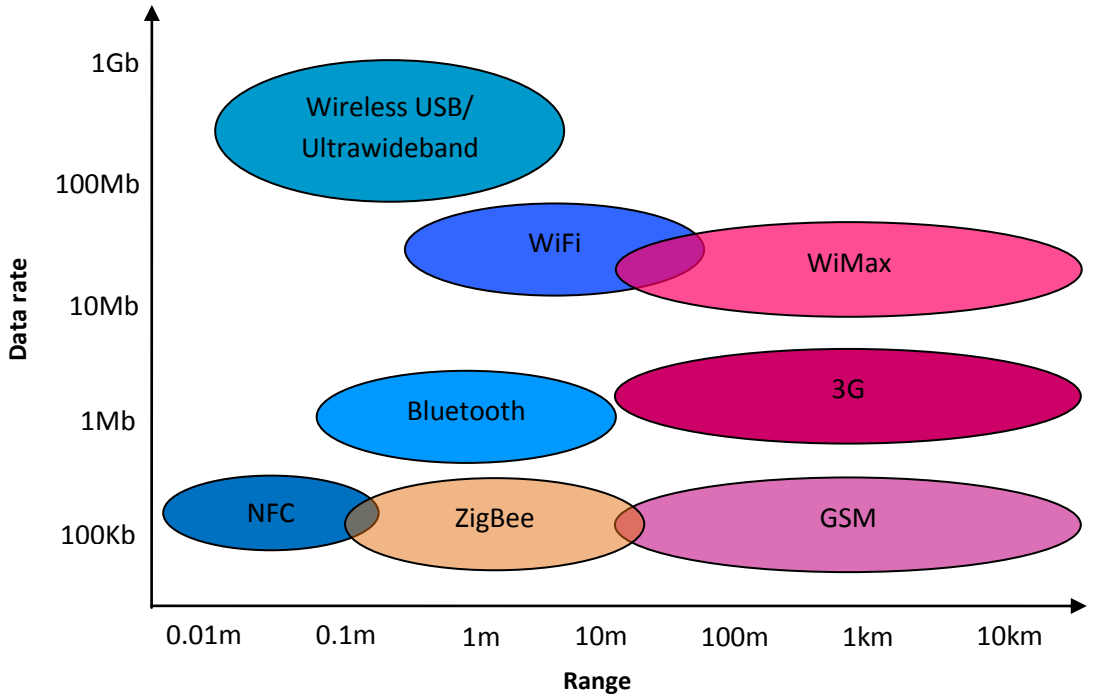
Bluetooth wireless technology allows computing devices to communicate with each other at a speed of up to 3Mbps with a maximum range of approximately 100 metres. Within a Bluetooth formed Personal Area Network (PAN), mobile devices can exchange information directly with each other, such as transferring data files, sending text or multimedia messages and connecting to headsets. In 2010, a total of 1.7 billion Bluetooth enabled devices (e.g. mobile devices, laptops and gaming consoles) were shipped worldwide (Bluetooth SIG, 2011). Moreover, 1.6 billion mobile devices were shipped and 64% of them were Bluetooth enabled (Communities Dominate Brands, 2010). In addition, statistics indicate that more than 70% of the mobile device users enable their Bluetooth connections during the day (Article Alley, 2010).

Some other technologies, such as NFC and Zigbee, are also at the forefront of wireless communication development. NFC technology supports two devices to communicate with each other within a very close rang (i.e. less than few centimetres). It can be utilised in many areas, such as access control, consumer electronics, information collection and exchange, and payment. Mobilecommercedaily (2010) suggested that 50 million NFC-enabled mobile devices would be commercially available in 2011. Also, according to the Juniper Research, mobile payment via NFC will generate $50 billion of revenue by 2014 (Knowyourmobile, 2011). Zigbee is a standard wireless technology which supports low-cost and low-power wireless sensors. The impact of Zigbee on mobile devices will be huge because of the level of sensitive information it accesses, such as secure mobile payment details and mobile office access control data (ZigBee Alliance, 2011). In addition, with over $1 trillion in revenue, Zigbee outsold all other wireless technologies in 2009 (Telecompaper, 2010).

USB is a technique for establishing a data connection between two computing devices with a maximum data rate of 180 Mbps. By using a USB cable, a mobile device can be connected with a desktop computer for exchanging information (e.g. data backups and synchronising with calendar schedules). In addition, a USB connection can be utilised for charging the battery of a mobile device. In 2009 alone, over 2 billion USB enabled devices were shipped (PC world, 2009). Compared with other aforementioned communication techniques, USB provides a more stable and faster connection for mobile devices but limits them to zero mobility.

The previous two sections described a number of mobile communication technologies that exist to date. Figure 2.3 illustrates the relationship between their data rates and their mobility. Although cellular communication technologies provide a safe and untethered environment to mobile users, their data throughput is somewhat limited. In comparison, other communication technologies

provide reliable and high rates of data exchange; however the mobile devices' mobility reduces significantly. In addition, how safely these technologies can be utilised is heavily dependent upon individual mobile users. It is not the author's intention to discuss the advantages and disadvantages for these technologies but to highlight their existence. Their availability affects mobile devices two-fold: by utilising various communication channels, mobile devices can provide many network based services; at the same time, this also creates a complex environment for deploying security controls anywhere other than on the mobile device itself.



Source: NFC Forum, 2011

Figure 2.3: Mobile communication technologies data rate vs. mobility

2.2.3 Mobile devices

Along with the rapid development of mobile communication technology, the mobile device has also experienced a dramatic evolution. Traditionally, people could only use the handset to make voice calls. Currently, the mobile has become a multimedia and multi-network computing device. Indeed, the mobile device operates similarly to a computer in terms of networking, processing power and data capacity. As demonstrated in Table 2.3, the iPhone 4, a typical mobile device which is commercially available, outperforms an average Personal Computer (PC) manufactured in 2001 in many aspects. Also, with a retail price of £520, 1.7 million iPhone 4 handsets were sold in the first three days when the device was first made available for purchase (CNET news, 2010).

Device	Iphone 4 (2010)	PC (2001)
Network	3G, GSM[1], WiFi, Bluetooth	LAN, Broadband
Memory	512 MB(internal)	256 MB (internal)
Processing power	Apple A4 800 MHz-1GHz	Intel Pentium III 800 MHz
Data capacity	32 GB	30 GB
Operation System	iPhone OS 4.2.1	Windows Millennium Edition
Market Price	£ 520	£1200

Table 2.3: Mobile device (2010) VS PC (2001)

At present, there are more than 5 billion mobile devices being used around the world. For the 2010 Q4 mobile device markets alone, a total of 101.2 million smart phones were shipped by various manufactures. The top five platform vendors were Google Inc., Nokia Corporation, Apple Inc., Research In Motion (RIM) Limited and Microsoft Corporation, with 32.9%, 30.6%, 16%, 14.4%, and 3.1% market share respectively (Canalys, 2011). As these smart phones are equipped with a number of communication network interface cards, a powerful CPU and massive data storage, they can provide a wide range of services and applications similar to that which a PC offers. By default, a number of common applications are preinstalled on the mobile devices by their manufacturers, such as: phonebook, clock and voice calling. In addition, mobile users can download and then install any other applications on the devices according to individual preference. This option completely changed the way that people utilise their mobile devices: from a dummy handset into a personalised computing gadget. Also, the more applications that are installed on devices, the greater the potential usage deviation is between various users. These mobile applications are designed by different vendors. Table 2.4 demonstrates a number of examples of application software stores. In total, there are more than 1 million applications available for people to choose from, across different mobile platforms. In addition, almost 15,000 new mobile applications become available for people to download every month (Distimo, 2010). Moreover, according to a white paper from Juniper Research, the mobile application global market is expected to triple from $10 billion in 2009 to $32 billion in 2015 (Juniper Research, 2010).

Application (App) stores	Established	Available Apps	No. of Downloads	Device Platform
Android Market	October, 2008	200,000	5 billion	Android
App store	July, 2008	500,000	15 billion	IOS
App World	April, 2009	38,000	1 billion	Blackberry
Ovi store	May, 2009	80,000	1.8 billion	Nokia

Table 2.4: Examples of App stores in 2011

[1] Global System for Mobile Communications

Each mobile application has a unique risk impact on the mobile system security based upon several criteria, such as their connection types, how much information they associate with, the nature of the information, their threat level and their vulnerability level. Based upon these criteria, Ledermuller and Clarke (2011) proposed the risk level which is associated with their application categories (as shown in Table 2.5). By employing the risk level of each application, their impact on the mobile system security can be observed: the higher the risk level an application has, the more impact it has on the system security. Therefore, various security controls can be applied for each individual application based upon their risk level: the higher the risk level an application has, the tighter the security control should be implemented for that application.

Application category	Application value	Threat level	Risk temp	Vulnerability level	Risk level
E-Mail (corporate)	8	4	8	2	8
E-banking	7	5	8	1	7
E-health	8	4	8	2	8
Remote access (corporate)	7	5	8	1	7
Remote access (private)	6	5	7	1	6
Voice communication	6	3	6	1	5
Stored business documents	6	3	6	3	7
Physical device	6	2	5	0	5
Personal information (online synchronized)	4	3	4	2	4
E-Mail (private)	4	3	4	2	4
Social networking	4	3	4	1	3
Messaging	3	3	3	2	4
Personal information	4	2	3	2	3
Web access (browser)	2	4	3	3	4
Stored documents	3	1	2	2	2
Maps & Navigation	2	1	1	3	2
News client	1	1	1	1	1
Utilities	1	1	1	2	1

Source: Ledermuller and Clarke, 2011

Table 2.5: Applications with their risk scores

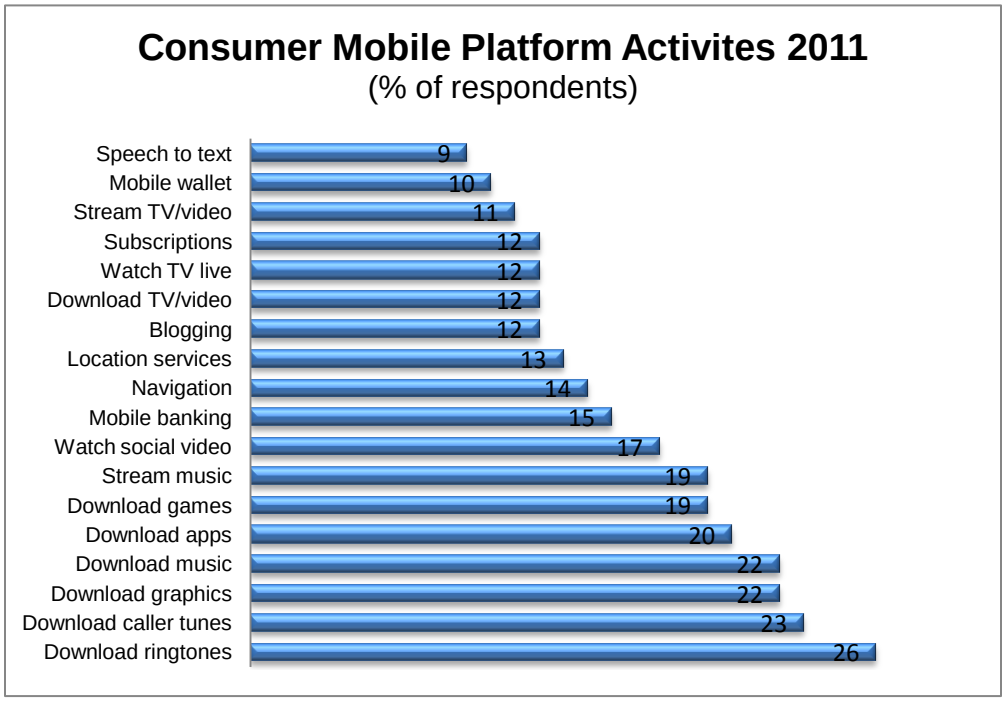
Table 2.6 illustrates a number of examples of both network based and host based mobile services which mobile users may use for a variety of purposes. For communication, people can send messages to each other through SMS, MMS, email and online messengers. In 2010, the mobile messaging market was valued at $179.2 billion. This number is predicted to increase to $209.8 billion by the end of 2011 and rise to $334.7 billion in 2015 (Portio Research, 2011). For finance, people can use Internet banking to check their account balance, transfer money and pay utility

bills. Also, by using the mobile NFC service, people can pay for goods at supermarket checkouts or vending machines. For instance, Orange and Barclaycard launched a mobile payment service which enables the users to pay for goods up to £15 (Aol tech, 2011). According to a research report of Berg Insight, there were 133 million mobile money users who made a total of $25 billion of transactions in 2010. Furthermore, they also predicted that with an annual increase rate of 40%, there will be 709 million mobile money users in 2015 with a total of $215 billion transactions (Berg Insight, 2011). Data storage enables people to store different kinds of information on a mobile device, such as personal contacts, calendar schedules, messages and documents.

Services	Network based	Host based
Voice	Make voice phone calls	Speech recorder
Data	Text message, multimedia message service, Emails, file transfer/sharing	Contacts, calendar, to do list, data storage
Multimedia	Video conferencing, GPS (Global Position System)	Music and movie player, taking picture and videos
Internet	Web browsing, Online messenger, mobile banking, mobile commerce	---
Others	Listen to the radio, watch TV programs, mobile NFC payment	Games, create documents, calculators, convertors

Table 2.6: Examples of mobile services

Figure 2.4 demonstrates the findings of a consumer mobile platform activities survey conducted by TNS mobile life (2011). In 2011, the top six user activities are related to data downloading. Moreover, 19% of the respondents communicate with their friends via social networking tools. Furthermore, mobile financial services, such as mobile banking and mobile payment grew strongly in 2011 compared with the previous year. In addition, Gartner (2009) predicted that among the top ten services a mobile device user would use in 2012, seven will be related to data downloading, mobile money and mobile communication.



Source: TNS mobile life, 2011

Figure 2.4: Consumer mobile platform activities 2011

As shown in this section, the functionalities of the device have increased in many aspects. This enables the mobile device to provide a wide range of services. Currently, people use these services to complete various tasks in their daily life. However, these tasks may be highly likely related to private personal information or critical business data. For instance, mobile financial services have to utilise bank account details of an individual to complete a transaction. Also, communication services may carry personal messages and customer information. Furthermore, as suggested by various studies, people store sensitive information on their mobile devices, such as passwords, bank account details, login credentials for personal and business email accounts, customer data and corporate intellectual property (Regenersis, 2009; BBC news, 2010; Kaspersky Lab, 2011; McAfee, 2011). Therefore, it is mission critical to ensure the legitimacy of a mobile user throughout every single session of usage. Otherwise, misuse would occur on both the services and information provided by the mobile devices.

2.3 Mobile device security threats

As demonstrated in the last section, the mobile device has become a powerful multimedia and multi-networking computing device. However, its ability is a double-edged sword. With mobile devices being able to host various services and store different information at the same time, this brings a number of security threats to the mobile environment, such as service fraud, Denial of

Service (DoS) attacks, malware and information disclosure (Stajano and Anderson, 1999; Viruslist, 2009; Muir, 2003). In this section, a comprehensive discussion will be given on mobile security threats.

2.3.1 Mobile service fraud

A mobile device provides many services through a telecommunication service provider network connection, such as voice calling, text messaging and web surfing. In order to utilise these services, a charge needs to be paid to the service providers. However, when a person uses such services without paying a charge, a service fraud occurs. For instance, when a mobile device is stolen, an unauthorised person could access the mobile services within a relatively small time frame until the owner of the device reports the incident to their service provider, who then has the power to terminate the connection. In order to maximise the window of opportunity for abusing the services, criminals could plot more sophisticated attacks which have a smaller footprint for detection, such as a Subscriber Identity Module (SIM) card cloning attack. By exploring the coding flaws within a cellular network authentication process, criminals could clone a victim's SIM card and abuse the services at the victim's expense (Rao *et al*, 2002). In this way, even at the end of a billing month, a mobile owner may not notice the abuse has occurred unless a thorough checking of their statements is undertaken. Moreover, criminals could launch a far larger scale of attack against the telecommunication service providers by using the SIM cloning trick. In 2010, the mobile operator O2 was hit by a multi-million pound fraud as a group of gangs cloned O2 SIM cards and called international premium rate telephone numbers (Which?, 2010). According to the Global Fraud Loss Survey 2009 of Communications Fraud Control Association (CFCA), service fraud is estimated to cost telecommunication service providers $72-80 billion every year around the world (CFCA, 2009). In addition, the number of fraud attacks has increased significantly by 74% between 2008 and 2009 (BBC news, 2009).

2.3.2 Denial of Service attack

Instead of abusing the mobile services, some criminals could plot DoS attacks to make these services unavailable to users. As a result, DoS attack is a security threat to the devices' availability. Within the mobile environment, a perpetrator could attack a mobile device or the networks it connects to with the launch of a DoS attack. The mobile devices rely on rechargeable batteries to function properly. By plotting a battery exhaustion attack, a mobile battery will be drained in a much shorter time than under normal usage (Stajano and Anderson, 1999). As the mobile devices use radio waves as a communication media, an attacker may use a signal jamming technique to

block the legitimate radio waves. As a result, all the network based services will become temporarily unavailable. Moreover, malicious attackers could disable a device completely over radio waves. For instance, attackers could use Bluetooth smacking which is a Ping-of-Death DoS attack to 'kill' a mobile device immediately (Browning and Kessler, 2009). Furthermore, as a mobile device is connected to the Internet, experienced attackers could plot a Transmission Control Protocol (TCP) flooding attack to stop the device from functioning properly (Swami and Tschofenig, 2006). Despite this there have not been any mobile DoS attack incidents reported yet, however, people should be aware of their existence.

2.3.3 Mobile malware

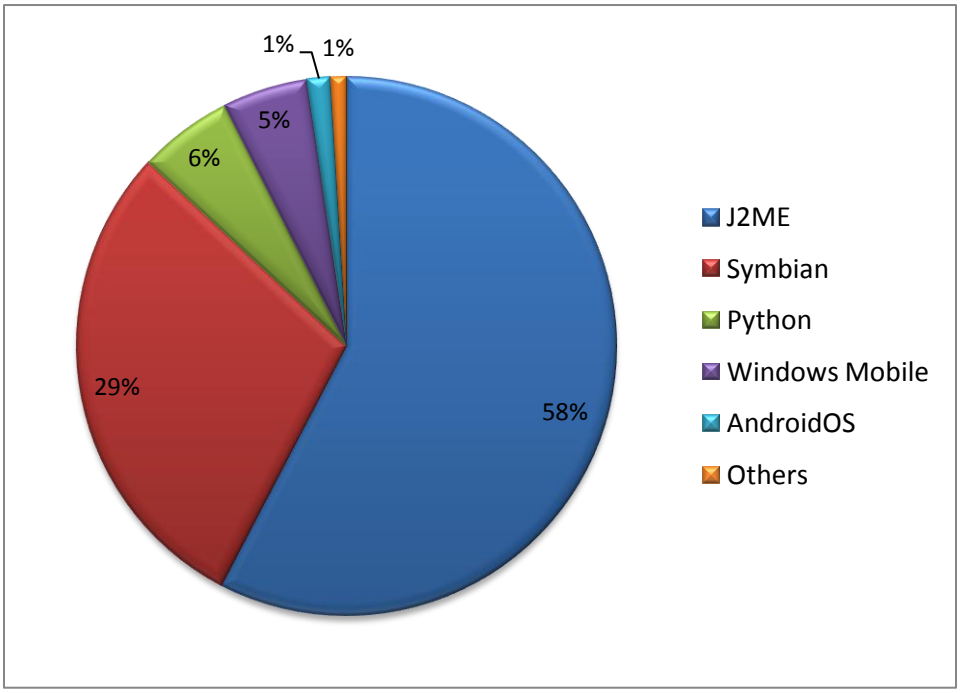
As described in the previous section, the modern mobile device has become much like a normal computer in terms of information processing, data storage and networking abilities. Unfortunately, mobile devices also face similar security issues which the traditional computers experience, such as malware. Malware stands for **mal**icious soft**ware**. It is designed to harm a computing system, harvest information or launch other types of attacks. The most recognisable malware are viruses, worms, spyware and Trojans. The first mobile device virus 'Cabir' was reported in June 2004 (BBC, 2004). Since then, the number of mobile malware increased steadily over the last few years. Indeed, by the end of 2009, there were more than 106 malware families with 514 variants identified (Securelist, 2009). Moreover, the number of new mobile malware being found in 2010 has increased considerably by 46% compared with those occurring in 2009 (McAfee, 2010). Furthermore, McAfee catalogued around 1200 unique mobile malware variants at the end of June 2011 (CSO online, 2011).

As demonstrated in Table 2.7, malware can affect the security of a mobile device at various levels. From simply duplicating itself to drain device batteries, to secretly sending SMS messages to a premium number; from basically changing a screen display, to remotely controlling a mobile device over the Internet. Mobile malware can be spread in many ways, such as through a Bluetooth connection, via a multimedia message or by embedding itself in a mobile application. Among these methods of proliferation, malware embedded in an application holds the largest potential threat. Once the application is downloaded and installed, the malware is also installed but without the owner's knowledge. For instance in 2010, up to 4.6 million Android users downloaded a suspicious application that secretly collected and transmitted users' information to a website in China (ComputerWeekly, 2010).

Threat levels	Malware	Effects
Low	Cabir	Constantly replicates itself through an active Bluetooth connection or removable media to drain the mobile battery
	Skulls.A	Allows the users to make or receive phone calls, all other applications are blocked and the screen is changed to display skulls
Medium	RedBrowser	Secretly sends SMS messages to a premium number
	Locknut.A	Blocks the phone and prevents any applications from opening
High	FlexiSpy	Sends call logs and copies of SMS/MMS messages to a secret server
	Brador	Allows a hacker to remote control the device via an Internet connection

Table 2.7: Example of Mobile malware and its effects

As illustrated by Figure 2.5, mobile malware attacks mobile devices regardless of their operating systems (OS). The number of malware for individual platforms highly depends upon their popularity of usage. As there are more than 3 billion Java 2 Micro Edition (J2ME) enabled mobile devices around the world (Java, 2011), the J2ME platform has become the top targeted platform by the malware creators associated with 613 variations of malware (57.67% of total malware). Despite the share of malware for the iPhone platform being significantly lower when comparing it with other platforms, the damage caused by the iPhone related malware can be severe. For instance, if an iPhone is infected by the iPhone/Privacy.A worm, attackers can gain access to the user's contacts and messages, and eventually steal a phone owner's identity (ZDnet, 2009).



Source: Securelist, 2011

Figure 2.5: The distribution of malware by platform

2.3.4 Social engineering attack

Social engineering attacks utilise emails or malicious websites to steal personal information and computer system login credentials by masquerading as a legitimate organisation. In the mobile environment, attackers can additionally utilise two techniques to solicit information: Voice call phishing (Vishing) and SMS phishing (Smishing). Normally, attackers make a voice call or send out a spam text message purporting to be from a financial organization. For example, attackers could call bank users with the following message "Your ATM card needs to be reactivated" and ask for their personal information. If the user is fooled by the Vishing attack, their information will be abused (FBI, 2010). Another example, early in 2011, a text message containing a phishing site was sent to customers of Bank of China as a reminder to reactivate their online banking tokens (McAfee, 2011a). If any customer clicked the phishing link, their login credentials (i.e. login ID, password and token) would be obtained and later abused by the attackers. Furthermore, the Smishing technique can also be used to plot other attacks. For instance, by simply replacing a phishing site with a link for a Trojan horse, if clicked, attackers could take the control of the mobile device without the owner's knowledge (PCWorld, 2006).

2.3.5 Loss or theft of the device

As mobile devices have always been high value computing gadgets, this consistently makes them prominent targets for attackers. Due to the small physical size and lack of physical protection that mobile devices possess, they can easily be lost or stolen. Indeed, according to the metropolitan police website, there are around 10,000 mobile devices lost or stolen in London every month (Metropolitan Police Service, 2011). When a mobile device is lost or stolen, there is an initial cost of replacement. More damage could occur if the attacker accesses the mobile services and information. For instance, the thief can make free phone calls, send multimedia messages and surf the Internet at the owner's cost. Also, as demonstrated in section 2.2.3 people do store sensitive information on their devices, such as bank details, login credentials for computer systems and emails, customer data and business plans. As a result, the attacker could also review all the information stored on the mobile device. Indeed, a survey shows that 32% of all information disclosure incidents were related to lost or stolen mobile devices (Ponemon Institute, 2011). Moreover, the McAfee mobile and security report indicated that "Four in 10 organizations have had mobile devices lost or stolen and half of lost/stolen devices contain business critical data", such as customer data, corporate intellectual property and financial information (McAfee, 2011).

Furthermore, such information can be used to perform other illegal activities and the damage is well beyond imagination. For instance, attackers could use the mobile owner's bank account login details to transfer money to their own bank accounts, or view a latest blueprint of product and sell it to the owner's competitors.

All of these aforementioned mobile security threats are considered as outside threats however security threats may come from inside as well. For instance, a colleague borrows a person's mobile device for making a voice call. Apart from utilising the telephony service, the colleague also has the opportunity to access other services or information, such as reading the owner's email messages, viewing the owner's social networking profiles, accessing the owner's document files or even installing malware on the device to capture the owner's call logs. Mobile devices lack the physical protection which other computing devices normally experience being kept within offices and homes which prevents these actions being carried out without the owner's notice. Such a security threat is also known as an insider attack. Comparing this with the aforementioned security threats, the insider attack is easier for attackers to plot and is more difficult for users to detect. According to the 2011 CyberSecurity Watch Survey, 21% of attacks on computing services and data were perpetrated by insiders compared with 58% by outsiders [2](Cert, 2011). Also, a Credant (2011) white paper suggested that 47% of security incidents were caused by insiders. Although the figures from the two findings are different, it is important to highlight the existence of insider attacks because they are just as dangerous as outsider attacks.

2.4 Mobile security controls

In order to counter the highlighted mobile security threats, various security projects have been proposed and developed. For instance, employing an authentication technique to stop unauthorised usage, using mobile antivirus products to detect and remove mobile malware, taking advantage of mobile firewall to filter unwanted traffic, utilising an encryption mechanism to protect the information stored on the devices, and making use of battery based mobile IDS systems to detect malware presence. These security controls will be discussed in the following section.

[2] The other 21% was unknown.

2.4.1 Authentication

A PIN is a knowledge based authentication technique. A user is required to enter the correct PIN before accessing a mobile device. Two types of PINs can be deployed: the first is for the mobile device itself and the second is for the SIM card. Normally, a mobile PIN contains between 4 and 8 digits. The PIN is a point-of-entry technique and is therefore only required when a device is initially switched on. Without the correct PIN, the device would not start and the SIM card would not authenticate with the cellular networks. However, most of the time the user will not be required to re-enter the PIN until the next reboot. This provides plenty of opportunities for attackers to abuse a mobile device. Recently, the use of the PIN technique has become more sophisticated; PINs can now be set to be requested again after a certain period of time dependent upon the user's preference. This would significantly reduce the possibility of the device being abused. Nonetheless, in practice, as many mobile users do not employ the technique properly, such as never changing the PIN, sharing it with friends or writing it down on paper, this makes the PIN based authentication technique inadequate as a protection of mobile devices (Clarke and Furnell, 2005; Kurkovsky and Syta, 2010).

With increasing hardware availability, a significant portion of mobile devices are equipped with new technologies (e.g. touch screens and built-in cameras). This provides opportunities for developing other authentication techniques on the mobile devices, such as the Android password pattern, a type of graphical password. Users are required to draw a shape on the 3 by 3 contact points on a touch screen as their password (as demonstrated in Figure 2.6). As users can only link two adjacent contact points together, this means the points which are not neighbouring with each other (e.g. 1 and 3) can never be used as a combination. As a result, the Android password pattern provides less password combinations than the traditional PIN based password technique can. In consequence, this method is more vulnerable to a brute force attack. As this method is also a knowledge based approach, it suffers several disadvantages as mentioned earlier, such as never being changed or being shared with others. In addition, research showed that this type password can be easily determined when a screen is greasy (Aviv *et al*, 2010).

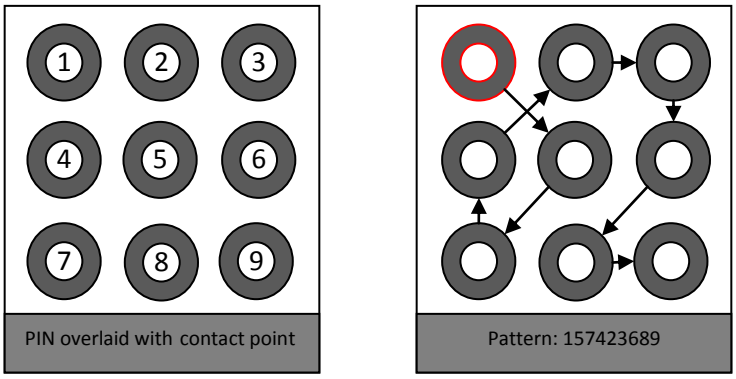


Figure 2.6: An example of Android password pattern

2.4.2 Mobile Antivirus solutions

Since the discovery of the first mobile phone virus in 2004, the antivirus software industry started to shift its attention from the traditional computing environment towards to the mobile platform. The first mobile antivirus software was developed by F-Secure and became available on the market in August 2005 (F-Secure, 2005). Since then, other antivirus companies also developed their counterparts, such as Kaspersky Mobile Security®, Trend Mobile Security® and Norton Mobile Security®. Mobile antivirus software was initially designed to detect and remove malware for the Symbian and Windows CE platforms due to their large market shares in the past. Latest mobile antivirus products also encompass other mobile platforms, such as Android based mobile devices because of its increasing popularity.

Just like traditional antivirus software, mobile antivirus software needs to update its signatures regularly to detect the latest malware. This process requires a dedicated Internet connection which was not available for mobile devices several years ago. However, with the growing availability of 3G and Wi-Fi technologies, it makes the updating process much easier and mobile devices could get the latest signatures promptly.

2.4.3 Mobile Firewall products

As mentioned in the last section, the mobile device could be exposed to various network based attacks due to its ability to access multiple wireless networks. In order to protect a mobile device from network based attacks, a mobile firewall software monitors the network traffic continuously and only allows legitimate services (e.g. web browsing) to go through a mobile device. Two types of firewalls can be implemented: on the network or on the mobile device. Nokia Corporation proposed a network based firewall which can be implemented on the mobile service provider's networks. It can be used for blocking malicious data going into a mobile device (Newscientist, 2007). As the filtering process is undertaken by the network service providers, there is no

overhead for mobile devices. However, it would be impossible for the service provider's firewall to protect mobile devices when they are connected with other networks such as Wi-Fi or Bluetooth. For the host based firewall, several security firms have already released products, such as ProtecStar Mobile Firewall 1.0 and Trend Micro™ Mobile Security 5.0 (ProtectStar, 2009; Trend Micro, 2009). As the firewall runs on the mobile device itself, it has the ability to monitor all networks that the mobile handset connects with. Nevertheless, due to the complexity of the multi-network environment, it is difficult to assess how well these host based mobile firewalls perform.

2.4.4 Mobile Encryption

Encryption techniques transform information to an unreadable format unless a key for the secured data is provided. As mentioned in earlier sections, mobile devices have the ability to store large amounts of information that could be related to both individuals and corporations. Without encrypting the information, anyone obtaining the device could access the information. In order to protect the information stored on the mobile devices, a number of encryption methods have been proposed. For instance, Microsoft Corporation offers encryption on Windows based mobile devices and RIM provides email encryption for the email system of Blackberry. Moreover, according to the Goode Intelligence mSecurity survey, 40% of organisations are planning to deploy data encryption methods on their mobile devices (Goode Intelligence, 2010). Nonetheless, encryption methods require a certain level of education for the average mobile device user before they can implement this technique.

2.4.5 Battery monitoring based mobile IDS

It is broadly recognised that the battery plays a key role in a mobile device. Depending upon the battery, the mobile device continuously provides various services. Several studies have identified that each mobile service consumes a unique amount of battery current (Martin *et al*, 2004; Jacoby *et al*, 2004). Based upon this theory, current usage of battery can be analysed. Two kinds of battery behaviour signatures can be created for detecting abnormal activities within the mobile device: for legitimate applications (e.g. calendar) or for malicious activities (e.g. malware).

To date, only Martin *et al* (2004) suggested that by using the legitimate services as the signature to prevent the battery exhaustion attack on mobile devices via the Power Secure Architecture (PSA). The main aim for the PSA was to protect the mobile device from three types of attacks: service request power attacks, benign power attacks and malignant power attacks. The PSA constantly monitors the mobile's battery usage level in order to obtain the battery signature of the current

running service, and then compares that signature with all trusted applications' signatures within a database. If no match is found in the database, possible power attack on the mobile device occurs and that service will be stopped immediately. The advantages of the PSA are: it detects possible power attacks to protect the life of the battery. Also it would possible detect malware attack. Nonetheless, as the system utilises the legitimate services to obtain the signature, it was reasonable as the number of mobile applications was limited in 2004. However, at the moment, there are millions of mobile applications available for the mobile users to choose. As a result, to obtain the signatures for legitimate service will not be an easy task. Even if all the signatures were obtained it would take too long to detect any intrusions. Furthermore, the system has not got the ability to detect any user related misuse, such as when the SMS service is abused by an attacker.

Comparing with the aforementioned method, the majority of the research employed the malicious software battery activities as the signature (as shown in Table 2.8). These systems frequently compare the present battery status with their signature database. If the battery signature of current activity matches with any signature of malicious software, the IDS system will stop that activity functioning. The advantages for battery based IDSs are that they are able to detect mobile malware and battery related attacks; hence, they protect the integrity and availability of mobile device. Also, they have a much lower false positive alarm rate and provide meaningful descriptions for each incident compared that which a behavioural based IDS system could offer. In contrast, obtaining and updating signatures can be a complicated task. A further limitation is that although battery based IDS systems monitor all running mobile applications' activities they cannot detect attacks which abuse legitimate applications, such as making an international phone call or data modification on the mobile device.

Name	Correlation location	Signatures types	Attacks can be detected
Martin *et al*, 2004	Host	Legitimate Services	Power attacks
Jacoby *et al*, 2004	Host and network	Common network attacks	Common network attacks
Jacoby *et al*, 2006	Host and network	Common network attacks	Common network attacks
Buennemeyer *et al*, 2008	Host	Common network attacks	Bluetooth network and Wi-Fi network attacks
Shabtai *et al*, 2010	Host	Mobile malware	Mobile malware

Table 2.8: A summary of battery based mobile IDS

Table 2.9 illustrates a comparison between existing mobile security mechanisms and mobile security threats. Although antivirus software can detect the presence of malware, firewall applications can block malicious network traffic, battery based mobile IDS can sense both malware and network related attacks and encryption can translate information to an unreadable format unless a secret key is provided, their abilities of identifying any user related activities are rather limited. For instance, they cannot determine the legitimacy of a user when a voice call is made or a file is accessed. Knowledge based authentication, such as using a PIN, can provide a basic level of protection for the mobile services and information being misused by unauthorised users. For example, without entering a correct PIN, a user will not be able to access any mobile services nor the information on the mobile devices. However, due to bad practice, such as choosing a simple password, never changing it, writing it on paper or sharing it with co-workers, unauthorised users are able to misuse the mobile device. Moreover, as the PIN is a point-of-entry based authentication method, as long as a correct password is given, a user will be granted access regardless of their true identity. In addition, this raises another issue with the knowledge based authentication approaches. When an authorised user forgets their PIN, they will be denied access despite their legitimacy. Therefore, none of the existing security controls can truly protect the multimedia and multi-networking mobile devices. As a result, a novel security control which can continuously protect both the mobile services and information based upon the users' legitimacy is desperately needed.

	Antivirus	Encryption	Firewall	PIN/Password	Battery based IDS
Mobile service fraud				✓	
DoS service			✓		✓
Malware	✓				✓
Social Networking					
Lost/stolen				✓	
Insider attack		✓			

Table 2.9: Mobile security mechanisms vs. Mobile security threats

2.5 Conclusion

With more than 5 billion users globally, mobile devices have become ubiquitous in our daily life. Mobile devices have the ability to provide various services across multiple communication networks and also on the handsets alone. People utilise them to complete different tasks, that are not only related to basic activities, such as making a phone call or playing games but also, more importantly, may involve sensitive information, such as storing personal data, transferring money

over the Internet and accessing corporate emails. As a result, the security requirement should be heightened to ensure the legitimacy of a user throughout the course of usage.

With the increased popularity of mobile devices, the associated threats are also increased from both outside and inside. For instance, the total occurrence of mobile malware has increased by 46% from 2009 to 2010 (McAfee, 2010). Another example, a survey conducted by the Ponemon Institute shows that 32% of information disclosure incidents were caused by loss or theft of the mobile device (Ponemon Institute, 2011). In addition, mobile services and information can be misused by a colleague when 'borrowing' a device. Several security controls, such as antivirus software, firewall applications, battery based IDS systems and encryption mechanisms, can be used to protect the mobile devices from being harmed by malware, network attacks and information disclosure attacks. However, their ability to detect user related activities (e.g. making phone calls and accessing information) is rather limited. Although the knowledge based authentication technique (e.g. PIN) could provide some level of protection against user misuse, its weaknesses have been well documented by literature (Clarke and Furnell, 2005; Kurkovsky and Syta, 2010).

As demonstrated in this chapter, the mobile device has the ability to access multiple networks and store a wide range of information and so it is critical to guarantee the legitimacy of user. Despite the antivirus, firewall and encryption applications that are already commercially available, their impact on monitoring user activity is minimal. The knowledge based authentication technique would provide a level of protection against unauthorised misuse. However, in practice, as the knowledge can be shared and learnt, this renders the method ineffective. As a result, a new security mechanism which can continuously assess the legitimacy of a user while the mobile services and information are used is definitely needed. The feasibility of utilising such a method will be discussed in the next chapter.

3 Review of Biometric Authentication

3.1 Introduction

To authenticate a person, three fundamental approaches can be used: something the person knows (i.e. password/PIN), something the person has (i.e. token) or something the person is (i.e. biometrics) (Wood, 1977). The first two authentication methods have frequently been utilised in security systems encountered in our daily life. In general, either of them can be employed if a system requires a basic level of protection. For instance, a password is required by a computer login system to prevent unauthorised usage; a user needs to swipe their ID card at their office building entrance to gain entry. When a system requires a higher level of protection, these two techniques can be deployed together to form a two-factor authentication method which provides stronger security than either of them could in isolation. For example, a user must provide both a password and possess a token to access their online bank account. However, these two techniques face a number of weaknesses in practice. Passwords can be forgotten, written down, shared with other people or even guessed by an attacker; tokens can be lost, stolen, borrowed by a colleague or cloned illicitly. In consequence, system security will be compromised and the system can then be abused by attackers. Therefore, an authentication method which can offer more robust security is needed and so attention has turned to biometrics.

Over the last 50 years, the development of biometric authentication techniques has increased dramatically: various biometric techniques have been extensively researched and some of them have already been developed for people to utilise. Initially, these authentication approaches were mainly utilised in areas requiring high security, such as governments and banks. Around the year 2000, biometric authentication techniques became more commercially viable and widespread in the public domain. For instance, a user can gain instant access to a computer system by swiping their finger on a scanner which is embedded in a keyboard or mouse. In another example, many countries have deployed a biometric passport system to verify the identity of a passport carrier based upon their biometric information.

3.2 An introduction of the biometric system

People use biometrics in their daily life despite the possibility that they may not be aware of its existence. For example, we can instantly identify our friends in a crowd through recognition of their faces; also, when we make a phone call to a friend, although we cannot see the person at the

other end, we can verify the identity of that person through their voice (either we know the person or we do not). However, within the computing environment, biometrics operates differently as the whole identification process is performed by a computer. In this section, a generic biometric system will be introduced along with various system performance measurement and requirement factors.

3.2.1 A generic biometric system

Biometric recognition or biometrics is an automatic process to uniquely identify humans based upon one or more physical (e.g. face) or behavioural (e.g. hand writing) characteristics or traits (Prabhakar, 2003). In the computing environment, a biometric system is mainly deployed as an authentication method for protecting the security of a computer system. In order to obtain system access, a user will be authenticated based upon the biometric information they possess.

A biometric system follows three distinct phases to perform an authentication process: enrolment, storage and comparison (as shown in Figure 3.1). Each step is performed by the following three main system components: a sensor, a computer and a classification method.

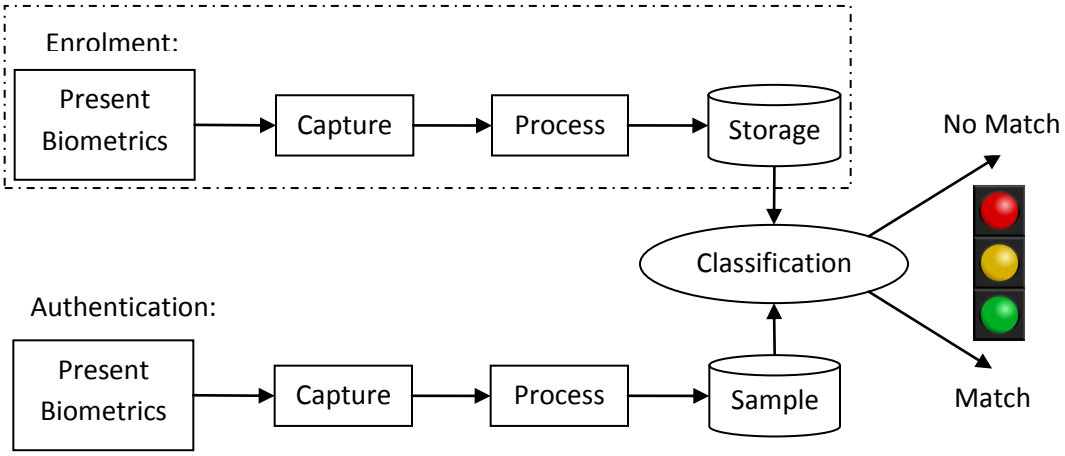


Figure 3.1: A generic biometric system

First of all, an individual user needs to enrol on a biometric system. During the enrolment process, biometric information of the user is captured by a sensor, then unique biometric characteristics are extracted, analysed and stored on a computer as a reference template. In subsequent usage, biometric information of a current user will be collected and compared with the reference template to perform the authentication process. Therefore, it is critical that the reference template information is obtained with a high degree of quality and accuracy. Also, some of the

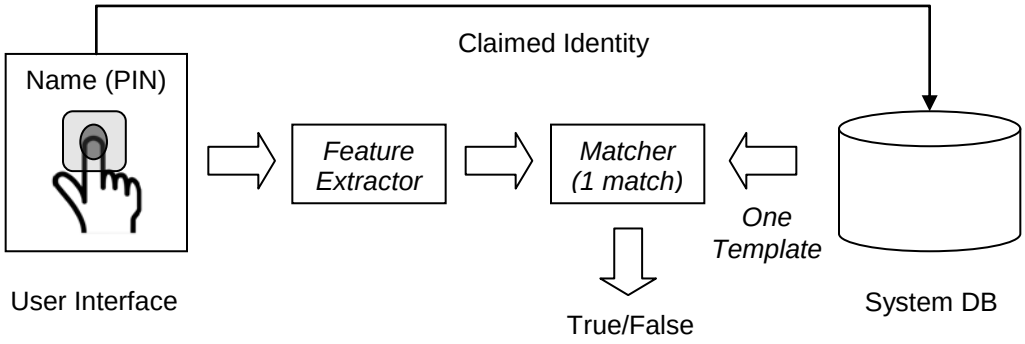
behavioural biometric characteristics (e.g. the way people walk) tend to change under various circumstances such as environmental factors. As a result, it is essential to update the template regularly to maintain a high level of system performance.

The authentication process compares an input biometric sample with the reference template sample(s). A current user's biometric information of is captured using a sensor and discriminate biometric characteristics are extracted, forming an input sample. Then, the input sample is compared with the template sample. The similarity between the two samples is calculated using a pattern classification method (e.g. a Neural Network) yielding an output value. Finally, the output value is compared with a predefined threshold: within the threshold, system access will be granted; exceeding the threshold, system access will be denied. It is important to choose a discriminatory system threshold. A poorly selected threshold will compromise system security by allowing imposters to enter the system too easily and system performance by denying legitimate users access to the system.

Depending upon whether a biometric authentication system is used to verify or determine the identity of a person, it can operate in two distinct modes: verification and identification.

- Verification: verifies an individual as the person who they claim to be (Am I who I claim I am?).
- Identification: identify who a person is (Who am I?).

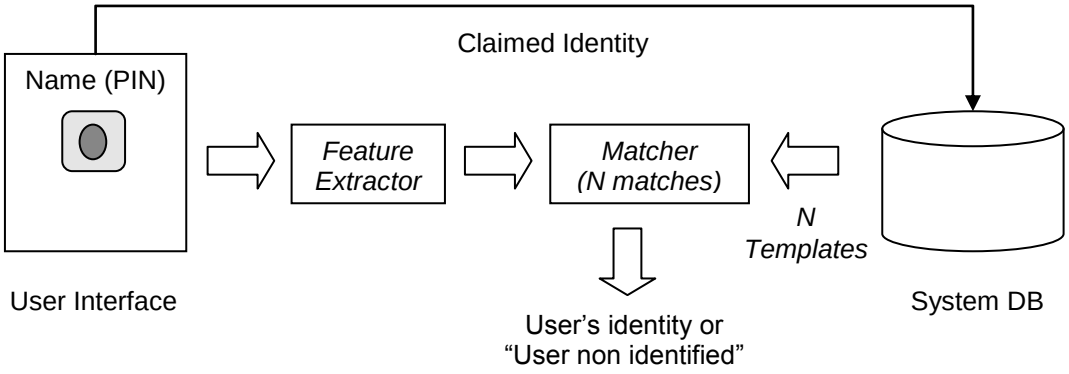
The verification mode is sometimes called one-to-one matching (as shown in Figure 3.2). It compares the biometric sample of a current user with the only reference template that contains the biometric sample of the claimed person. The comparison output is either true or false. For example, a fingerprint enabled computer login system operates in verification mode. When a user attempts to access the computer, their fingerprint sample is compared with the owner's fingerprint sample only. If the samples match with each other the user will be granted access, otherwise they will be refused.



Source: Jain *et al*, 2004

Figure 3.2: A biometric verification process

In identification mode, a current user's biometric sample of a current user must be compared with every single template on the system database to determine if a match exists. Therefore, the process is also known as one-to-many matching (as shown in Figure 3.3). At the end of the comparison process, the identity of the user can be either reviewed or the user cannot be identified. For instance, when the police need to ascertain if a suspect has broken the law before or not, the biometric information of the suspect (e.g. fingerprint) is compared with the templates in a database of known criminals. Another example, in the US, before a person claims social services benefit, their biometric information is checked on the system database which contains samples from people who have already claimed the benefit, enabling the detection of fraudulent claims. So far, 90,000 people have been enrolled on the benefit system of the social service (GlobalSecurity, 2011). This means the biometric information of an honest applicant would be checked against 90,000 templates before they will be awarded their claim for benefit. Compared with the verification mode, the identification mode is a more complex process as it requires more time and computational power to complete. More importantly, the biometric traits employed in an identification system need to be highly unique. As a result, behavioural traits (e.g. gait) are not recommended as candidates for any identification systems.



Source: Jain *et al*, 2004

Figure 3.3: A biometric identification process

3.2.2 Biometric system performance measurement factors

As mentioned in the last section, a biometric system identifies the legitimacy of a user based upon the comparison between the biometric sample of the current user and the existing reference template. For a particular biometric technique, the performance of the template matching process is reflected by two important error rates: False Acceptance Rate (FAR) and False Rejection Rate (FRR).

- FAR: is the probability that a biometric system incorrectly matches a biometric sample with a non-matching template. It measures the percentage of how many imposters are incorrectly accepted by the system.
- FRR: is the probability that a biometric system fails to match the biometric sample of a user with a matching template. It measures the percentage of how many legitimate users are incorrectly rejected by the system.

As shown in Figure 3.4, these two rates share a mutually exclusive relationship: as one rate decreases the other increases. As a result, the security level of a biometric system can be controlled by adjusting the threshold setting. A tightened system security level can be obtained by increasing the FRR; this means fewer attempts will be granted with the system access. While by increasing the FAR, the system security level is slacker as more attempts will be granted access.

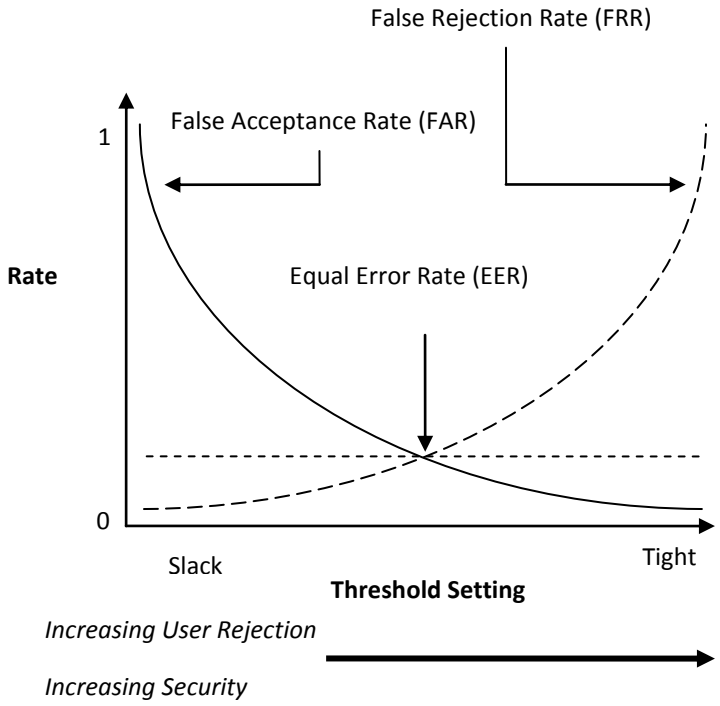


Figure 3.4: Mutually Exclusive Relationship between FAR/FRR

To compare the performance of various biometric techniques, a universal measurement parameter such as the Equal Error Rate (EER) can be employed. The EER is an average value obtained from the FAR and the FRR. It is the point at which the FAR and FRR are equal, when they cross each other as in Figure 3.4 or the smallest distance between these two rates when they do not cross. To acquire the EER for a particular biometric based authentication system, a number of participants are invited to test it and their individual EERs are recorded. The average EER from all the participants is then calculated and this final figure signifies the EER for the system. As a result, the performance of a biometric system is heavily reliant upon the number of participants, the uniqueness of each participant and the sophistication of the employed classification method. In general, a biometric technique with a smaller EER tends to be more accurate.

When designing a biometric authentication system other performance parameters such as the failure to enrol rate, failure to capture rate and the template capacity, should also be taken into consideration. When the failure to enrol rate of a system is high, users have to make more effort to be successfully enrolled on the system. If the failure to capture rate is high it suggests that there may be an equipment problem and so an alternative sensor can be used to replace the original. The capacity of the template also needs to be considered as identification based biometric systems hold more than one user's biometric information.

3.2.3 Biometric system requirement

People have a large number of biometric characteristics and traits, such as face and gait. If a biometric characteristic or trait can be utilised for an authentication system, it should meet the following criteria (Jain *et al*, 2004):

- **Universality**: requires that every single person should have the characteristic or trait. For instance, people have got fingers; hence the fingerprint has the potential to be used as a biometric identifier.
- **Uniqueness**: examines how well a biometric technique discriminates people from each other: a person's fingerprint is much more unique than their hair colour, but less unique than their iris.
- **Permanence**: indicates how constant a biometric characteristic remains over time. The fingerprint of a person never changes, however, the way they walk will change due to their age, fitness level, footwear and even the weather conditions.
- **Collectability:** how easy it is to collect the biometric sample. Using a normal camera a facial image can be taken within a couple seconds, however to obtain an iris image users have to stare at a special infrared camera for a much longer time.
- **Performance**: refers to how well a biometric performs: its accuracy, speed and robustness.
- **Acceptability**: indicates at what level people are willing to use biometrics as an authentication method in their lives. People would prefer a fingerprint scan compared with an iris scan as the latter technique is more intrusive.
- **Circumvention**: refers to how easy a system can be tricked by using a substitute. A fingerprint scan system can be fooled using a fake finger; while it is difficult to trick a facial thermograph based authentication system with a replicated face as the system has the ability to detect whether the face is live or not.

As a result, an ideal biometric authentication system should fit all the above requirements.

3.3 Biometric characteristics

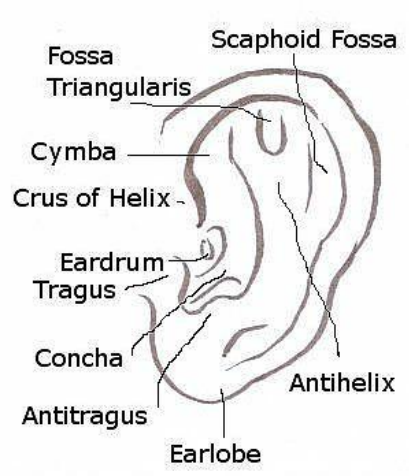
Based upon characteristics, biometric systems can be subdivided into two categories: physiological and behavioural. The physiological characteristics are related to the shape of the human body, such as face, fingerprint and iris. In contrast, behavioural characteristics are the ways in which the human body behaves, such as how an individual writes a letter (i.e. hand writing), how they walk

(i.e. gait) from one location to another and how they speak (i.e. voice). Over the last 100 years, significant amounts of effort have been spent on a variety of biometric projects. This section will describe these biometric methods both in the research field and related commercial applications.

3.3.1 Physiological biometrics

The physiological biometric based systems utilise the characteristics of a human body part to identify individuals. In general, physiological biometric characteristics are resistant to various factors which may affect their performance. For instance, people's fingerprints will not be affected by their age, mood, body fitness or the weather conditions. Moreover, an individual's physiological biometric characteristics contain high levels of discriminatory information. For example, a person's iris is so unique that even identical twins have different iris patterns. Research into physiological biometric approaches started in the late 1800's and primarily focused on the usage identification via fingerprint. Since then, many other studies into various physiological biometrics have been performed.

Ear recognition examines the shape of the outer human ear as a means of identifying individuals (as shown in Figure 3.6). In 1949, Alfred Iannarelli conducted the first experiment in which he studied the uniqueness of human ears. By manually studying more than 10,000 random hand drawn pictures of human ears, Iannarelli suggested that the human ear shape is unique even for biological twins (Iannarelli, 1989). Later, the Iannarelli System was developed to identify individuals through their ear shape based upon 12 measurement points, such as the concha and lobe areas. Burge and Burger (2000) described the potential of using ear recognition in the computing environment. Their approach utilised the features extracted from the Voronoi diagram of the human ear to identify individuals. Other research also suggested that ear recognition is a reliable technique to discriminate people through 2D or 3D images (Yuan and Mu, 2007; Yan and Bowyer, 2007). Currently, the majority of ear recognition work is carried out in the research arena.

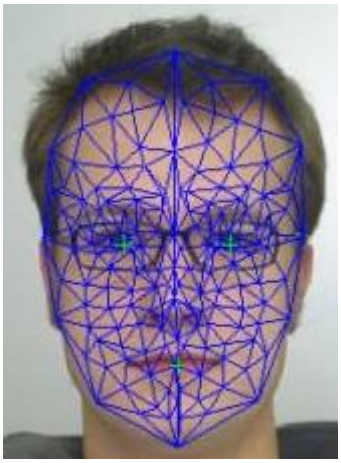


Source: Advancedsourcecode, 2011

Figure 3.5: An anatomical sketch of a human ear

In general, ear recognition techniques can provide a reliable and robust identification method for individuals. Additionally, this approach is considered as user convenient as the ear image can be taken from a distance. Nonetheless, in several circumstances, it may be difficult for an ear recognition system to carry out the identification process, for instance when an ear is covered by an object (e.g. ear rings) or inconsistent lighting impedes the capture of an image of suitable quality. However, Burge and Burger (2000) suggested that by employing an expensive infrared camera, a certain level of identification can still be obtained by capturing a thermogram ear image.

Facial recognition is a technique to identify and verify people through their faces. The research into facial recognition started in the 1960s despite humans having naturally used the face to identify each other throughout time. Bledsoe (1966) and Goldstein *et al* (1971) identified several unique characteristics from human face photographs to distinguish people, such as the distance between the eyes, width of the nose, the shape of cheekbones and the depth of eye sockets (as shown in Figure 3.7). Since then, many related research projects have been proposed. Although each research project may choose the facial features differently, most of the projects employed one of the following three popular methods to perform the classification: Principal Component Analysis (PCA) (Turk and Pentland, 1991), Linear Discriminant Analysis (LDA) (Etemad and Chellappa, 1997) and Elastic Bunch Graph Matching (EBGM) (Wiskoot *et al*, 1997).



Source: Geekosystem, 2011

Figure 3.6: An example of face recognition

Victor *et al* (2002) and Chang *et al* (2003) identified that facial recognition based systems perform better than ear recognition based systems do. As a result, facial recognition techniques can also be deployed for use as both identification and verification solutions. The facial recognition technique is user friendly because a face photograph can be taken from a distance without any user interaction. As a result, the identification process can be performed secretly without the user's knowledge. The major drawback of facial recognition approaches is that system performance can be significantly affected when a poor quality photo is taken. For example, when the face is covered by glasses or a person is too far away from the camera when photographed. In addition, it is arguable that the human face shape may change over time and so the system template should be updated accordingly if necessary.

Currently, facial recognition techniques have been developed by many vendors and used for many applications (Face-rec, 2011). For instance, the AxxonSoft (2011) facial recognition based surveillance system can identify a particular person amongst a large crowd. Toshiba have introduced a face recognition based login system on their new laptops which enables users to quickly logon to their laptops by presenting their faces to the in-built camera rather than typing their passwords (Toshiba America Information Systems, 2011). So far, facial recognition techniques have been the fastest growing sector among all the biometric approaches (Free-press-release, 2011). Moreover, the facial recognition market is expected to grow by 24.2% from 2010 to 2015 (marketsandmarkets, 2011).

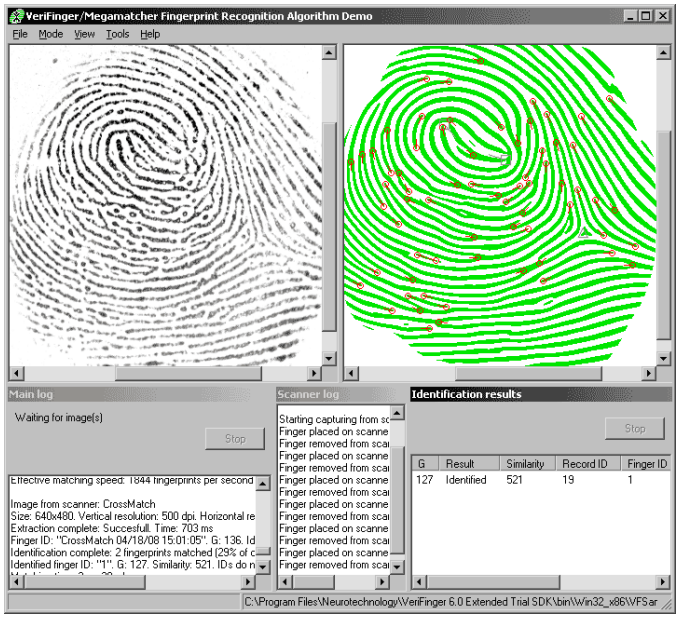
Facial thermography uses the heat patterns emitted by blood vessels under the skin of the human face to identify individuals (as shown in Figure 3.8). The heat pattern is also known as a

thermograph which contains strong discriminate information (Prokoski *et al*, 1992). Apart from the image being captured by an expensive infrared camera, the facial thermography technique works similarly to facial recognition based approaches. The advantage of the facial thermography technique is that it is not an intrusive approach; as the image can be taken from a distance, users are not required to make any physical contact with the camera. In addition, as the image is obtained by an infrared camera, this permits the technique to work perfectly in a dark or no light environment. However, the performance of the system could be affected by several external factors, such as surrounding temperature (Socolinsky & Selinger, 2004). Furthermore, due to the high manufacturing cost, this technique could only be used for high-level security requirement applications (e.g. government intelligence sectors) but not for a wide public deployment.

Source: Socolinsky & Selinger, 2004

Figure 3.7: An example of human face thermo image

Fingerprint recognition relies on the patterns of friction ridges and valleys of the human finger to distinguish individuals (as shown in Figure 3.9). The uniqueness of fingerprints has never been doubted: *"Two like fingerprints would be found only once every 10^{48} years"*-Scientific American, 1911. Research on fingerprint recognition can be traced back in the late 1800's as Galton developed a fingerprint classification system by employing all ten human fingers. Later, based upon Galton's work, Henry (1900) proposed a detailed fingerprint indexing method for assisting manual fingerprint comparison. The method is known as "the Henry system" which laid the foundation for the majority of existing work in the fingerprint recognition domain. Trauring (1963) proposed an automatic comparison method to identify individuals by using finger ridge patterns. Since then, many research studies have been conducted in this area.



Source: Neruotechnology, 2011

Figure 3.8: An example of Fingerprint Recognition

A fingerprint recognition system requires the user's fingerprint image to perform the identification. Traditionally, a finger image was obtained when a person covered their finger with ink and pressed it against a piece of paper. Today, the fingerprint acquisition process is much easier. To capture a user's fingerprint, one of the following hardware sensors can be utilised: capacitance, optical, thermal and ultrasonic. Users are required to swipe their fingers against the sensor and then the fingerprint image is automatically generated. During the image processing stage, various unique features are extracted from the image. Based upon individual system preferences, these features are classified by using one of the following methods: correlation based, pattern based and minutiae based. Correlation based algorithms superimpose two fingerprint images together and correlate between corresponding pixels to calculate the difference between alignments. The pattern based matching compares the raw fingerprint patterns (i.e. arch, loop and whorl) from two fingerprint images which have to be aligned in the same orientation. The minutiae based method extracts a number of minutiae points from the fingerprints, such as the ridge endings and ridge bifurcations, to form two dimensional graphs. The difference between these graphs can then be analyzed.

Fingerprints are so unique and consistent over time and can therefore be used for both identification and verification. For identification, the technique is frequently used by the law enforcement agencies to identify currently unknown suspects against various databases of known criminals. For verification, the technique can be deployed as an alternative login method for

computer systems (e.g. laptops). Nevertheless, the system performance could be significantly reduced when the finger is covered by dirt or has suffered a small cut. Moreover, people find this technique rather intrusive as it requires users to physically swipe their finger across a sensor to capture the image.

Fingerprint recognition is one of the most well-known and used biometric techniques. So far, it has been developed in many applications for the purpose of authentication, such as computer login systems, physical access control for office buildings and attendance tracking solutions (EyeNetWatch, 2011). Currently, with $1.37 billion estimated revenue in 2010, fingerprint recognition based applications hold the largest biometric market share. In addition, the future fingerprint biometrics' market is promising as its expected revenue will reach $3.28 billion in 2015 (marketsandmarkets, 2011).

Hand geometry utilises a number of the human hand geometrical shape features such as the thickness of the palm, width of the fingers and length and the distance between knuckles, to discriminate people. The research into hand geometry started in the early 1970s. Although limited literature was produced on the topic at that time, a number of patents were filed describing how hand geometry based systems work (Ernst, 1971; Sidlauskas, 1988). In order to obtain the image of the hand geometry, two approaches have been proposed. Traditionally, a hand geometry system required users to place their hands in a fixed position by using pegs on a scanner (Jain *et al*, 1999; Sanchez-Reillo, 2000) (as shown in Figure 3.10). As a result, the scanner can easily locate the human hand and generate the hand image accordingly. As the pegs may affect the quality of the image, Covavisaruch *et al* (2005) suggested another method which allows users to freely put their hands on a scanner without having the pegs. Later, the hand geometry characteristics (e.g. thickness of the palm) are located using pre-designed computer software. Despite various classification methods being employed by different systems, they all examine a similar set of hand geometry features (Duta, 2009).

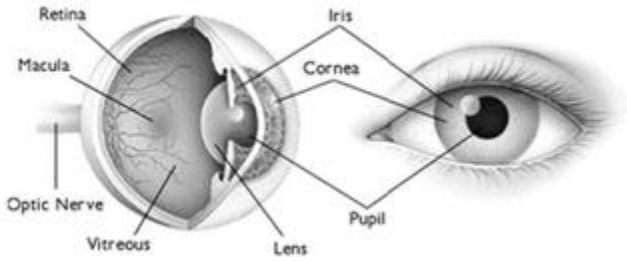
Source: Clevelandtime, 2011

Figure 3.9: An example of hand geometry scanner

Due to the natural similarity of human hand shape, hand geometry features are not highly unique. As a result, this technique can only be used to verify people but not to identify them. With its ease of use and stand-alone capability, it is widely deployed for many verification applications, such as physical access control and class attendance tracking (A.T.R. Systems, 2003). Furthermore, people find this technique is less intrusive than fingerprint recognition based approaches. The major downside of hand geometry based systems is that the technology is restricted for a wider spread of usage due to its bulky size (e.g. cannot be used on laptop computers). In addition, the system is not suitable for children as their hand shape changes quickly over time.

Iris recognition identifies users by examining their iris. The iris is the coloured muscle surrounding the human eye pupil and it is highly unique to each individual person (Daugman, 1993) (shown in Figure 3.11). In order to obtain an iris image, one of the following types of camera is used: near infrared (NIR), high-resolution visual light and telescope-type. Once the iris image is acquired, locating the iris area can be a difficult task as a poorly selected iris area will reduce system performance. Iris recognition is a highly accurate and stable technique which is 10 times more accurate than fingerprint recognition based systems could get (EPIC, 2005). As a result, the technique can be deployed for both identification and verification. Also, this technique is less intrusive as the image can be taken from a distance of up to 3 metres (Du, 2006). As there is no physical contact with the camera, the iris scan can be performed safely and hygienically. However, the system does require users to align their eyes with the camera which may cause a certain level of inconvenience. Moreover, the initial cost for the equipment can be very expensive, especially for long range cameras. As a result, iris recognition technology should only be implemented for applications requiring high security. Indeed, one of these applications is the Iris Recognition Immigration System (IRIS) which is currently being deployed by the UK Border Agency in several

airports, such as Heathrow, Gatwick and Birmingham. Passengers can be quickly verified by IRIS and then pass the barriers within a couple of minutes, whereas the process is much longer without an IRIS implementation (UKBA, 2011). Furthermore, the market for iris recognition is expected to grow 25.4% between 2010 and 2015 (marketsandmarkets, 2011).



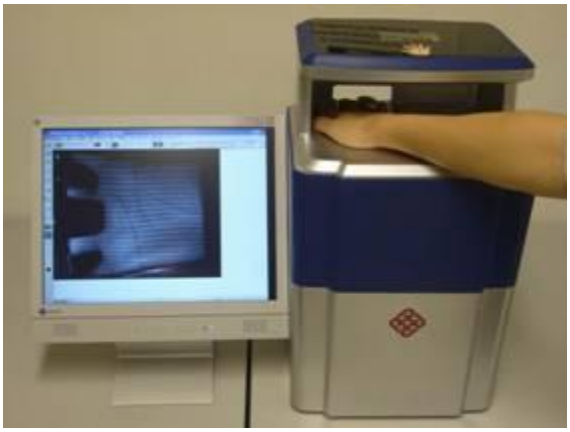
Source: Itimes, 2011

Figure 3.10: An example of a human eye

Retina scanning: the retina is formed by the nerve tissues located at the back of the human eye (as shown in Figure 3.11). Retina scanning examines the unique pattern formed by the blood vessels of the retina. The pattern is so unique that retina scanning based identification systems can achieve an error rate of 1 in 10 million which is 10 times better than the performance of iris recognition based systems (Wisegeek, 2011). In addition, it is extremely difficult to replicate or forge the pattern of the retina. As a result, the technique is considered as the most secure biometric approach. However, retina scanning is a very intrusive process. A user has to remove their glasses (if they have any), put their eyes close to a scanner and stare at a specific point for approximately 10-15 seconds until the scanning process is completed. Also, as the technique requires a laser or infrared scanner to scan the human eyes, this may raise health and safety issues. Furthermore, due to the high cost of implementation, the technique is mainly deployed for maximum security requirement areas, such as governments, banks and the military (Biometric Newsportal, 2011).

Palm print recognition relies on the patterns formed by the principal lines, wrinkles and ridges on the palm inner surface to identify individuals (Shu and Zhang, 1998). It works similarly to fingerprint recognition. Users are required to physically put their hands on a scanner in order to allow the palm print to be generated (as shown in Figure 3.12). Then the image is analysed mainly by one of the following methods: Line-based approaches, Subspace-based approaches and Statistical approaches (Kong *et al*, 2009). The advantages for palm print recognition are that rich discriminatory features can be extracted from the large palm area. Also the approach is accurate

in performance and ease-of-use for users (Sun *et al*, 2005). Nonetheless, it is an intrusive approach as physical contact with the scanner is required from users. Currently, most of the palm print recognition work is still research based. Zhang *et al* (2003) and Fong and Fong (2008) suggested the technique can be used to identify people for online applications (e.g. e-banking) and consumer products (e.g. computers).



Source: PolyU, 2009

Figure 3.11: An example of palm scanner

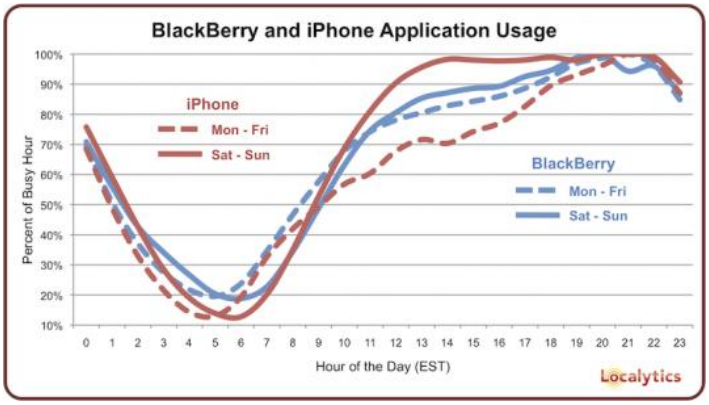
Apart from the aforementioned physiological biometrics techniques, other physiological characteristics such as body odour, fingernail bed and hand veins, have also been proposed and investigated as alternative discriminative methods to distinguish individuals in the future (Bhattacharyya *et al*, 2009).

3.3.2 Behavioural biometrics

Behavioural biometrics identifies a person based upon their unique behaviour, such as the way they walk. Human behaviour can change over time due to various reasons; aging, fitness, social networking environments and weather conditions are all examples. As a result, the discriminatory characteristics also tend to change, affecting the performance of any behavioural biometric system based upon these indicators. Nonetheless, the impact can be minimised if the template is regularly examined and updated. Compared with physiological biometric techniques, behavioural based methods are less unique but more flexible and user-friendly. In this section, a number of behavioural biometric approaches will be discussed in detail.

Behaviour profiling identifies people based upon the way they interact with their computing devices and how they use their computing services/applications. For instance, a user's identity can be verified through the way in which they utilise their mobile devices: which applications are

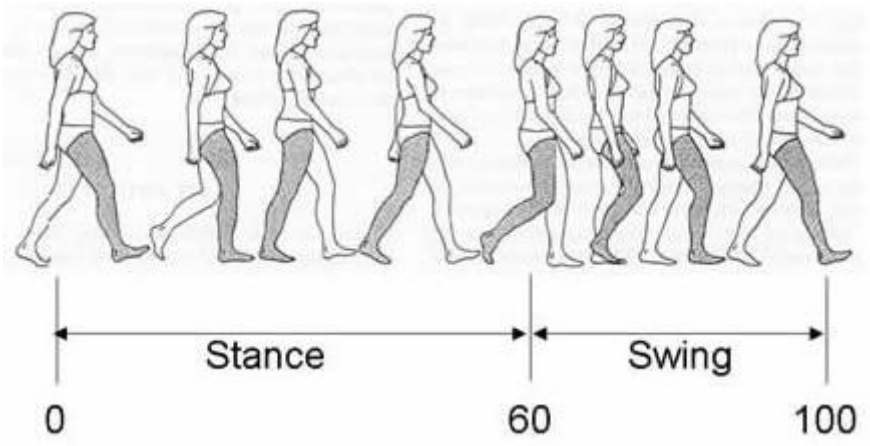
utilised and where and when the device is used (shown in Figure 3.13). In addition, other factors provide distinctive attributes contributing to the identification process, such as the networking and processing activities of the device. In a behaviour profiling system, a current user's behavioural activities are compared with an existing template (which is obtained from historical behavioural usage) by using various classification methods (e.g. a Neural Network). The user identity is determined based upon the comparison output. Behaviour profiling systems can provide continuous and transparent identification while users interact with various computing services or applications. However, compared with other behavioural biometrics, the template of a behaviour profiling system contains larger variations and requires a longer time to form.



Source: Intomobile, 2010

Figure 3.12: BlackBerry and iPhone average Application Usage comparison

Gait recognition employs a sequence of human limb movement to identify an individual. Gait motion can be obtained using a camera or video recorder (images can be extracted from the video) in the form of a sequence of pictures (shown in Figure 3.14). Alternatively, the gait motion can be collected by utilising an accelerometer. Then, this gait information is analysed using one of following approaches: model based and motion based (Xu *et al*, 2006). In the model based approach, gait sequences are represented using model parameters, while in the motion based approach, body movement is considered as one entity without employing any models.



Source: Queen's University, 2011

Figure 3.13: Gait cycle

In general, human gait contains a level of unique characteristics which can be used to discriminate individuals. As the gait images are obtained from a distance without any user physical contact, a gait recognition based system is a non-intrusive approach. However, a person's gait could change over a long period of time due to their age, body weight or fitness. In addition, gait can be influenced by other factors, such as the weather, footwear, ground conditions and personal emotions. As a result, the performance of a gait recognition based system can vary. Gait recognition applications could potentially be used for video based intelligent surveillance systems to verify people's identity in the future (Lu and Zhang, 2007).

Handwriting recognition: Handwriting has been used as a means of identification for hundreds of years despite the identification process being manual. The handwriting recognition process was fully automated in the late 1980s (Plamondon and Lorette, 1989). For a handwriting recognition system, the identification process can be carried out in two distinct modes: dynamic (on line) or static (off line) (Das, 2007). A dynamic system approach examines how handwritten words are produced such as the stroke order, writing speed and pressure. Conversely a static system compares obtained handwriting images with existing templates. Forging static handwriting images can be easily done, however to dynamically replicate someone's handwriting is extremely difficult. The majority of users find this technique nonintrusive as they sign documents all the time. Nonetheless, because people may change their handwriting over time, this method can only used for verification purposes. Currently, a number of commercial handwriting based applications are available, such as customers signing on Personal Digital Assistants (PDA) when goods are received and users authenticating themselves on a handwriting recognition enabled mobile device via a stylus (as shown in Figure 3.15).

Source: Canvas Solutions, 2011

Figure 3.14: An example of a handwritten signature on a computing device

Keystroke analysis: keystrokes describe the action when a person interacts with a computer keyboard. Robinson *et al* (1998) demonstrated that keystroke activities show a level of uniqueness between different users. Two main features can be extracted from keystroke activities: inter-keystroke latency (the elapsed time between releasing the first key and pressing the second) and hold-time (the total amount of time that each key is pressed down) as demonstrated in Figure 3.16. The process of identifying people by their keystroke features is known as keystroke analysis (or keystroke dynamics). The identification can be performed in two modes: static (text dependent) and dynamic (text independent). In the static approach, a user's typing pattern is examined when certain keys are pressed (e.g. when entering a password). A profile is obtained when they repeatedly enter the same characters several times until a satisfactory system performance is reached. In the dynamic approach, a user is verified based upon their overall typing pattern (e.g. the typing rhythm speed). A different method is used to acquire the profile for the dynamic approach: the user enters a number of typing samples with different text allowing a profile template to be formed.

Source: BioPassword, 2007

Figure 3.15: An example of keystroke analysis

The advantage of keystroke analysis (static mode) is that it can provide an additional layer of protection to existing password based access control mechanisms. For instance, BioPassword, an existing commercial product, requires users to type their user names and passwords in a precise way to be logged into a system (Times Newspapers, 2007). As users are familiar with the password entering process, there is no additional requirement for them. The dynamic keystroke analysis approach can provide transparent and continuous verification of users while they work on such tasks as writing a report or composing an email message. Moreover, no additional hardware is required as the technique is embedded within the keyboard system. The major downside of keystroke analysis is that it is like other types of behaviour based approaches; it can only be used for verification purposes but is not unique enough to be considered as an identification solution.

Voice verification is also known as speaker recognition. It is based upon the way people speak to identify individuals. Although the voice is a physiological trait that utilises a combination of several body vocal tracts (i.e. the mouth, nose and throat) to function, voice verification is mainly based upon the study of how individuals speak (i.e. voice speed and speaking accent). As a result, voice verification is commonly classified as a behavioural biometric (Woodward *et al*, 2003). Unlike voice recognition systems, voice verification systems focus on *who* is speaking rather than *what* a person says. In voice verification systems, the analogue human voice is converted into a digital format and various voice features (e.g. pitch, cadence and tone) that can then be extracted and formed into a voiceprint. Similar to keystroke dynamics, voice verification can also operate in two modes: static (word dependent) and dynamic (word independent). Static voice verification systems require a user to speak a predefined phrase which is also known as the “pass phrase”. As a result, it can be mainly used as a point-of-entry technique. Dynamic voice verification systems do not require any pass phrases to identify a user. Instead, systems continuously monitor their speech behavioural characteristics (e.g. rhythm). Hence, it can be deployed as a transparent

verification method: verifying a speaker's identity during a telephone conversation. The advantage of voice verification is that it can be used for both verification and identification purposes (Campbell, 1997). Also, in most cases, no additional hardware is required for implementing voice verification technology as most mobile devices are equipped with microphones. Nevertheless, any changes in the human voice may impact upon the performance of a system, such as surrounding temperature, mood, medication and physical change of the vocal tracts.

The above two sections discussed the majority of known biometric techniques to date. In general, the physiological biometric techniques provide more discriminative information but these methods are intrusive as they require some level of physical contact with users. In contrast, as behavioural biometrics characteristics tend to change over time, behavioural based approaches perform better in verification mode than they do in identification mode. Further, behavioural based techniques are user friendly and less intrusive and they could continuously and transparently verify people in the background.

Based upon the biometric system requirements mentioned in section 3.2.3, Jain *et al* (2004) conducted a brief comparison of all the aforementioned biometric approaches as presented in Table 3.1 (H, M and L represent High, Medium and Low respectively). Table 3.1 shows that none of the biometric approaches outperforms any of the other approaches based upon all seven requirements. For instance, retina scanning is highly unique and extremely difficult to forge but people find it hard to accept this technology due to its level of intrusiveness. In comparison, the behaviour profiling based approach tends to have very high acceptability because of its transparent nature, however its permanence is much poorer as a user's behaviour is likely to change over time.

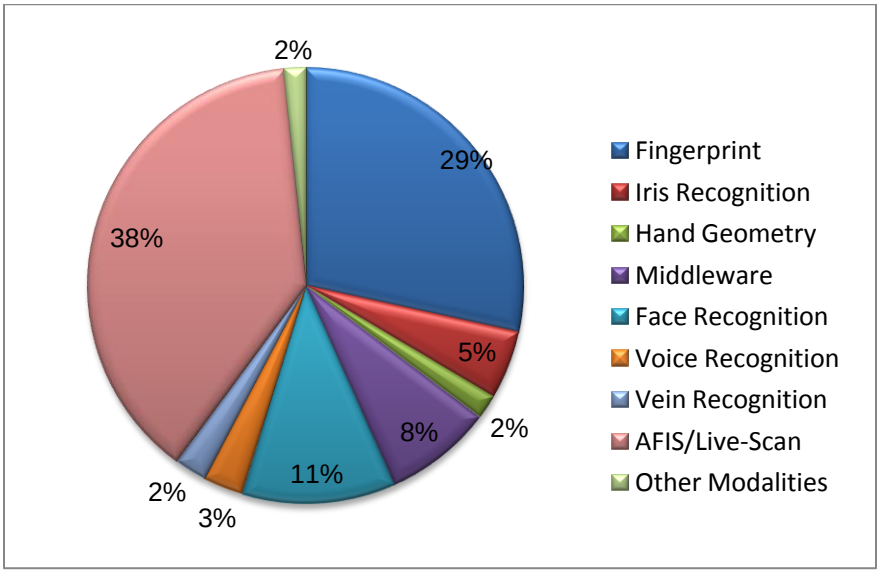
Biometric approach	Universality	Uniqueness	Permanence	Collectability	Performance	Acceptability	Circumvention
Ear recognition	M	M	H	M	M	H	M
Facial recognition	H	L	M	H	L	H	H
Facial thermography	H	H	L	H	M	H	L
Fingerprint recognition	M	H	H	M	H	M	M
Hand geometry	M	L	L	H	L	H	M
Iris recognition	H	H	H	M	H	L	L
Retina scanning	H	H	M	L	H	L	L
Palm print recognition	M	H	H	M	H	M	M
Gait recognition	M	L	L	H	L	H	M
Keystroke analysis	L	L	L	M	L	M	M
Handwriting recognition	L	L	L	H	L	H	H
Voice verification	M	L	L	M	L	H	H
Behaviour profiling [3]	M	L	L	H	L	H	H

Source: Jain *et al*, 2004

Table 3.1: A brief comparison on biometrics approaches

Figure 3.18 illustrates the biometric market share by revenue for various technologies in 2009. It clearly demonstrates that the physiological based technologies dominated the biometric marketplace while the behavioural based technologies had less than 5% of the total market share. With a total of 66.7% market share (38.3% for Automated Fingerprint Identification System (AFIS) and 28.4% for other fingerprint identification system), fingerprint based systems were found to be the most popular biometric technology in 2009. Face recognition and iris recognition technologies were also popular with 11.4% and 5.1% market share respectively.

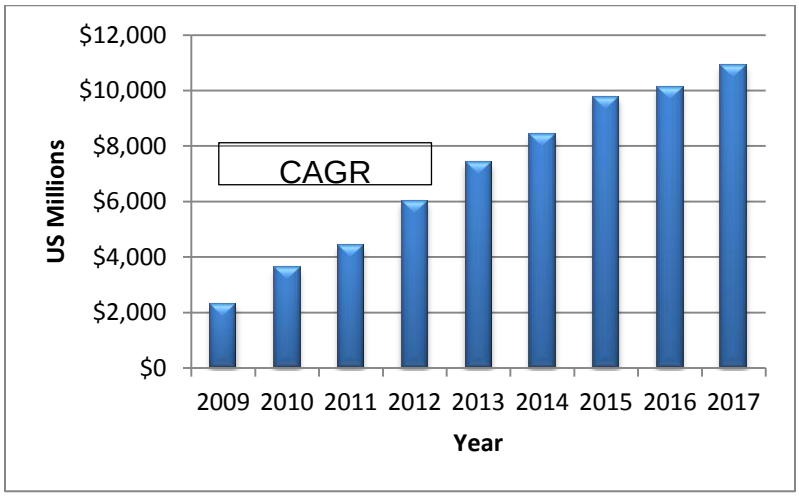
[3] Inserted by author



Source: International Biometric Group, 2009

Figure 3.16: Biometric Revenues by Technology

Figure 3.19 demonstrates the predicted revenues for the biometric industry from 2009 to 2017. With a forecasted Compound Annual Growth Rate (CAGR) of 19.69%, the global biometric industry is anticipated to experience strong growth through 2017 and beyond. Also, according to Securitynewsdesk (2011), the forecast for revenue within the biometric market in 2015 is $14 billion. Although the figures are slightly different from each other, the fact is that the biometric market is predicted to grow strongly year on year and that biometric techniques will play a significant role in the future.



Source: Acuity Market Intelligence, 2009

Figure 3.17: Biometric Industry Revenues

3.4 Biometric approaches applicable for use on a mobile device

As demonstrated in the last section, research into biometric approaches is rapidly maturing and commercial biometric development for access control (both behavioural and physical) grows significantly year on year. With increasing computational power and hardware availability, the chance to adopt biometric based access control approaches on mobile devices is becoming more realistic. As highlighted in Figure 3.20, some mobile devices already possess a number of inbuilt features capable of sensing a variety of user biometric traits, enabling several approaches to be easily deployed upon them.

Figure 3.18: Biometric approaches on a mobile device

Behaviour profiling as described in Chapter 2, the modern mobile device provides a variety of network and host based services. It is arguable that people utilise these mobile services differently. For example, when a user accesses their mobile calendar service to find out what their daily schedules are, the features related to this behaviour are the time of access (7:15 AM), the duration of access (1 minute) and the day of access (Monday). However, when an attacker accesses the same service, they are likely to choose a time when the owner does not normally use

the device (e.g. 3 AM) and the duration of access might be much longer (e.g. 5 minutes) as they want to explore as much information as possible. As the attacker's activity deviates from the user's normal behaviour profile, a security monitoring system could detect the incident. To the author's best knowledge, there has not been any research conducted into behaviour profiling for mobile devices.

Face recognition most modern mobile devices are equipped with an inbuilt camera which is designed for taking pictures, shooting videos and making video conference calls. This creates the opportunity to use facial recognition/ear recognition on the mobile device. In addition, by utilising an expensive infra-red camera, iris recognition and retina scanning could also be permitted. Weinstein *et al* (2002), Al-Baker (2005) and Clarke *et al* (2008) proposed a thin-client based topology for face recognition on mobile devices. A user's facial image was captured using an inbuilt camera and then sent to a network server for further processing (i.e. comparison with the template and reviewing the user's identity). Depending upon individual approaches and their datasets, their system accuracies fell in the range of 79%-95.6%, highlighting the potential of developing facial recognition for mobile devices.

Fingerprint recognition**:** is the first biometric approach that has been deployed on mobile devices as an authentication method. In 1998, Siemens and Triodata developed a fingerprint recognition prototype by placing a sensor at the back of a mobile phone (Bromba, 2011). By utilising the prototype, a user can gain instant access to the phone by swiping their finger against the sensor instead of entering the password. Since then, many fingerprint recognition based authentication systems have been developed and implemented on various mobile devices by different manufacturers (Mainguet, 2011).

Gait recognition: When a user carries their mobile device in their trouser pocket, their gait information can be collected as they walk. Derawi *et al* (2010) employed a Google G1 mobile phone with an inbuilt accelerometer to gather a carrier's gait activities. Their experimental result was 20.1% EER when testing 51 volunteers' gait activities. This indicates that gait recognition shows some level of discrimination for mobile device users. However, a substantial improvement is required in this technique before it can be considered for wider deployment.

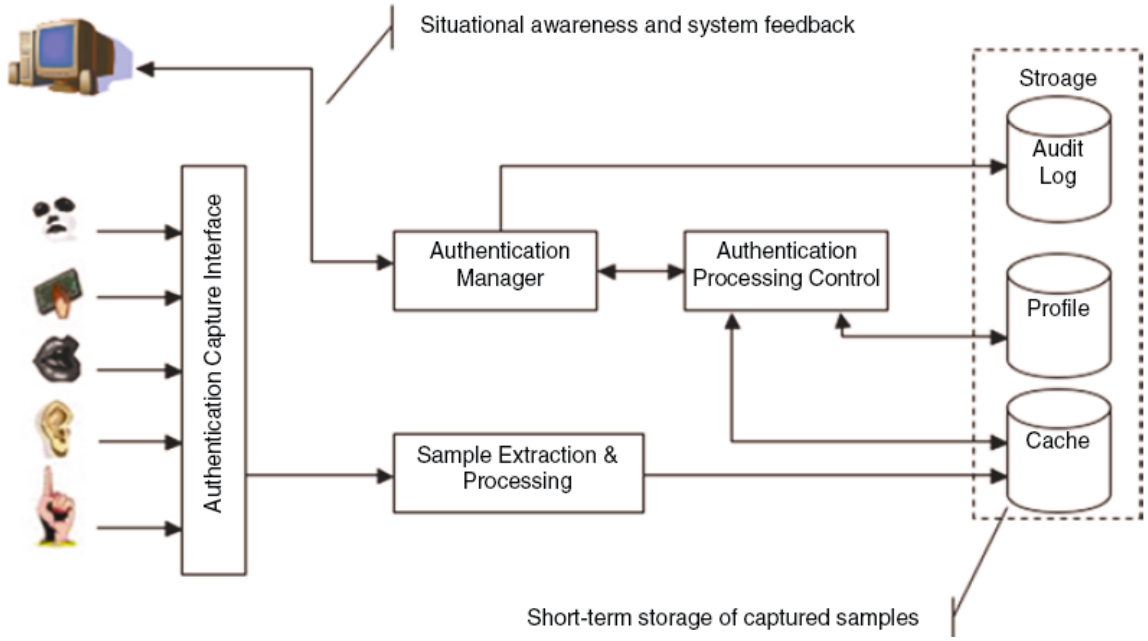
Handwriting recognition: a significant proportion of mobile devices have been equipped with a touch screen, enabling the handwriting verification technique to be deployed. A user's identity can be verified when they perform their signature (static) or while they write a message by using a

stylus (dynamic). Clark and Mekala (2007) proposed a dynamic approach to verify a user when certain words were written. With a 1% EER, their system performance was better compared with other behavioural techniques. Despite their approach not being fully dynamic as the words were pre-chosen, their work demonstrated that it is possible to identify users based upon the way they write on a mobile device.

Keystroke analysis: While people are typing a text/email message or entering a password, their keystroke activities can be used for keystroke analysis (both static and dynamic). Several research projects were proposed to explore the possibility of using keystroke analysis on mobile devices, such as Clarke and Furnell (2006) (both static and dynamic), Buchoux and Clarke (2008) (static) and Campisi *et al* (2009) (static). With an average 13% EER, keystroke analysis based authentication systems can be deployed in practice to provide an extra layer of security for mobile devices.

Voice verification: Traditionally, mobile devices were primarily used for making telephone calls, during which a user's voice sample can be captured for the purpose of voice verification. Woo *et al* (2006) examined the possibility of using static voice verification for the mobile device by using an ASR-dependent speaker verification approach. Despite the comparison process being carried out by a standard computer, their work achieved a 7.8% EER proving that a mobile device user's identity can be verified by their voice, even in a noisy environment (e.g. in a busy office).

By utilising various biometric techniques, the TAS authenticates mobile device users in a continuous and transparent manner as shown in Figure 3.21 (Clarke, 2011). The TAS chooses individual biometric techniques to verify a mobile user based upon the configuration of their mobile device. For instance, if a mobile device is not equipped with an inbuilt camera, the TAS will only choose keystroke analysis and voice verification to verify the user. One example for TAS is the Non-Intrusive and Continuous Authentication (NICA) (Karatzouni *et al*, 2007). By utilising the combination of various biometric techniques, NICA can achieve an EER less than 0.01%.



Source: Clarke, 2011

Figure 3.19: A generic TAS framework

Many of the applicable biometric approaches have achieved a good level of performance and some of them have already been utilised by the mobile security industry. In general, based upon the way they provide security, they can be put into two categories: point-of-entry and transparent based systems (as shown in Table 3.2). For the point-of-entry based techniques, they only verify the users' identity at the beginning of a session. Once the user obtains the initial trust from these techniques, their legitimacy will never be challenged again. In comparison, transparent based approaches work in a similar manner to IDSs; they constantly check the users' identity throughout usage, even when a user has successfully passed point-of-entry authentication. As Chapter 2 identified, a new security system needs to provide continuous protection throughout a usage session. As a result, the point-of-entry based biometric techniques will not be employed by core functions of the new security mechanism; but they might be used by the new security mechanism when a strong authentication technique is required. For transparent techniques there are behaviour profiling, face recognition, gait recognition, handwriting verification, keystroke analysis and voice verification; all of which can be implemented on mobile devices to provide continuous and transparent protection. Face recognition can easily verify users when they make a video call or partake in a video conference. However, on other occasions, the verification process cannot be easily performed because of the difficulty of capturing high quality facial images. Gait recognition authenticates users when they walk from one location to another but it is impossible to perform when they are stationary, such as sitting in front of an office desk or lying in bed. Keystroke

analysis and handwriting recognition examine users when a message is composed or a document is modified. However, little protection can be provided if a user views a webpage or reads a document. For voice verification, a user can only be authenticated during a conversation. Therefore, with all these activity based techniques a user's continuous protection will become exhausted when a particular activity does not occur.

Biometric approaches	Point-of-entry	Transparent
Behaviour profiling		✓
Face recognition	✓	✓
Finger recognition	✓	
Gait recognition		✓
Keystroke analysis	✓	✓
Handwriting recognition	✓	✓
Voice verification	✓	✓

Table 3.2: Biometric approaches on mobile devices

The behaviour profiling technique verifies users based upon the services/applications they use. As a result, this approach provides truly continuous protection to users unless they do not interact with the mobile device at all. Although little research has been conducted into the behaviour profiling technique within the mobile host environment, significant amounts of research suggest that mobile device users can be discriminated between each other via their calling behaviour and migration behaviour through service providers' networks.

3.5 Literature review on behaviour profiling

The research into mobile behaviour profiling started around 1995, focusing mainly upon the area of IDS to detect telephony service fraud. Three mobile user activities have been studied so far: calling activity, migration mobility activity and migration itinerary activity (both the mobility activity and itinerary activity are user's location activities and are defined in the following subsections). To date, all behaviour based mobile IDS systems are network based, as users' behaviours are obtained and monitored by network services providers.

3.5.1 Telephony service based mobile IDS

The telephony based mobile IDS monitors a user's calling attributes (e.g. international Mobile Subscriber Identity (IMSI), start date of call, start time of call, duration of call, dialled telephone number and National or International call) to detect service fraud, SIM card cloning and the loss or theft of devices (Moreau *et al*, 1997). By collecting these features over a period of time, a historical calling usage profile can be acquired. If the deviation between a current calling session and the historical profile exceeds a predefined threshold, an intrusion is identified. There are a

number of telephony based mobile IDS systems and they will be introduced in the following section.

The earliest work on telephony service based detection systems was the European Advanced Security for Personal Communication Technologies (ASPECT) project on mobile security (Gosset, 1998). The ASPECT project covered different security aspects within mobile communications such as authentication, encryption and service fraud detection. A number of techniques were used to study a user's calling behaviour, such as supervised neural network and unsupervised neural network (Lerouge *et al*, 1999). The evaluation process was carried out by several experimental studies on a dataset which was collected from the Vodafone network. The dataset contains a total of 317 fraudulent and 20,212 legitimate users. Their experimental results were a detection rate of 50% and a FAR of 0.02%..

Samfat and Molva (1997) proposed an Intrusion Detection Architecture for Mobile Networks (IDAMN) which provided multilevel protections for mobile GSM networks. The multilevel protection is applied to each user across three levels: velocity and clone verification, component wise verification and intrusion detection. The architecture monitors the user's behaviour in terms of both telephony and migration activities. A mobile user's telephony activity is divided into two statistical vectors, call vector and session vector. The call vector is a local parameter that measures all outgoing calls and the session vector is a global parameter that measures the following activities; total number of calls, total duration of calls, network connection duration and total number of handovers within a period of time. By using this information a profile and a threshold can be obtained. If a current vector value is bigger than the threshold an alert is raised to a network administrator. The IDAMN was evaluated by using a simulation method. Four types of users were simulated: domestic, business, corporate and roamer. In general, call vectors had a lower false alarm rate of 1% compared with a 2% false alarm rate for session vectors. However session vectors had a better detection rate of 90% compared with a 70% detection rate for call vectors. The session based approach had a better detection rate because over a long period of time, an intruder's activity deviates more than a legitimate user's behaviour. Among these four categories, business users had the best performance with an average detection rate of 89% and a false alarm rate of 1.5%.

Boukerche and Notare (2002) described a service fraud detection model on the mobile phone system using a Radial Basis Function (RBF) neural network model. By using user calling features, the model can detect possible call service fraud. In addition, the model employed a smart

procedure: once a possible fraud is identified, an alert will be sent to both the individual user and network administrators immediately, rather than at the end of a billing month. The experiment dataset was collected by an unnamed telecommunication service provider and contains 4,255,973 telephone calls. A variety of experiment configurations have been tested with combinations of call features and RBF neural network setups. Their lowest system error rate was 4.2% and was achieved using 110 neurons in the hidden layer of the RBF neural network.

3.5.2 Migration based mobile IDS

A user's migration activity is the way that they travel from one location to another. There are two types of migration activities: mobility and itinerary. By calculating the possibility of a mobile user travelling from one mobile cell to another, migration mobility based mobile IDS systems could detect telephony service attacks. If the result exceeds a predefined threshold, a possible intrusion is detected. Whilst similar to migration mobility based mobile IDS, migration itinerary based mobile IDS systems also monitor cells to detect telephony service attacks. Instead of monitoring one cell at a time, migration itinerary based mobile IDS systems monitor all cells a user covers during their journey from one location to another. It is believed that people always have the destination in their mind when they travel and so certain routes will be chosen as regular or favourite routes. As a result, the probability of mobile users travelling over these routes is much higher than them travelling through other routes. To extend this, when an attacker carries other people's mobile devices, the route they take is likely to be different to the owners' route.

3.5.2.1 Migration mobility based mobile IDS

The IDAMN (Samfat and Molva, 1997) also monitors the user's migration pattern to detect intrusions for the telephony service. A user's migration mobility activity can be obtained when mobile users traverse from one cell to another. Using this information, their mobility profile can be generated and is maintained when the location updating procedure of the mobile device occurs. By using a mathematical formula, a predefined threshold is derived using historical mobility information. The architecture is evaluated via a simulation method for four categories of users: domestic, business, corporate and roamer. The results show that domestic users achieve the best system performance with a false alarm rate of 2% and a detection rate of 90%. In comparison, due to frequent travel plans, the roamers have the worst system performance with a false alarm rate of 7% and a detection rate of 65%.

Buschkes *et al* (1998) propose an anomaly detection method for GSM networks by using the Bayes decision rule. The Bayes decision rule is a mathematical model which calculates the probability of a current activity occurring based on prior activity. Another method is outlined in their work to aid comparison with the Bayes decision rule; the average algorithm. The average algorithm calculates the Mean Residence Times that a mobile carrier stays in one cell. Using the Mean Residence Times and when the mobile carrier enters the cell, a user's mobility profile can be built. Two scenarios are analysed: town and motorway. The results show that: in the town scenario, the prediction rate for the Bayes rule model was more than 80% after 5 days and it reaches 83% after 15 days monitoring; for the motorway scenario, the prediction rate of the proposed model reached 94% after 5 days and was more than 95% after 15 days.

Sun *et al* (2004) propose a mobility-based anomaly detection model for cellular mobile networks by utilising the combinations of the following techniques: high order Markov model, Ziv-Lempel data compression algorithm and Exponentially Weighted Moving Model (EWMA). The high order Markov model was used to calculate a mobile user's mobility probability from one cell to another. In order to store this mobility information for each individual mobile user, the Ziv-Lempel data compression algorithm was employed to create a mobility profile. Also, the EWMA technique was utilised to efficiently update the mobility profile. Therefore, a more accurate user profile can be regularly updated. The system constantly compares a mobile user's current mobility action with their mobility profile to detect possible intrusions. Once the comparison value exceeds the threshold, an alert is then generated to notify a network operator. The evaluation process of this model was created using a simulation method in the following environment: a cellular network containing 40 cells, each having six neighbours on average and the average distance between two cell towers is 1 mile. The simulation results show: the false alarm rates of the system were around 25% and 5% when a user travels at a speed of 20 miles/hour and 60 miles/hour respectively. Also, when a user's speed is 20 miles/hour, the system detection rate is 80% and this reaches almost 95% when a user travels at 60 miles/hour. At a higher speed, the mobile carrier covers more cells than at a lower speed and so the deviation between an attacker and the legitimate user will get accordingly larger.

Two major questions are raised regarding their system performance: what are the detection and false alarm rates the system experiences when the mobile carrier's speed is less than 20 miles/hour? What kinds of people are suitable for the system to monitor? For the first question, their results indicate that both the detection rate and false alarm rate were poor if the speed was

less than 20 miles/hour. For the second question, the majority of pedestrians, if not all of them, experience an average speed of less than 2 miles/hour which is much less than 20 miles/hour; furthermore, when people drive in the city, the speed is limited to 30 miles/hour for most areas, with traffic lights and safety islands, the average driving speed would be around 20 miles/hour, which is the worst case in the simulation result.

By aiming to improve the performance of the system, several modifications have been made to the existing model, such as adding Sharon's entropy theory to adjust the system threshold (Sun *et al*, 2006). Therefore, the new system not only has a constantly updated profile but also a frequently modified threshold. Furthermore, two profiles were created for each mobile user: weekdays and weekends. The evaluation of the system is executed using a simulation method. The experiment results show that the average false positive rate for the adaptive mechanism is reduced by around 7% compared with the non-adaptive method. In general, the adaptive mechanism had a slightly better average detection rate than the non adaptive mechanism did. However, when a mobile carrier's speed was at 20 miles/hour, the adaptive mechanism had a much higher detection rate with around 7% improvement over the non-adaptive mechanism. The advantages of the modified system are: a better detection rate and a lower false alarm rate due to adapted profile and threshold settings. On the other hand, the improved Intrusion Detection system still has a similar problem as the previous version: both the detection rate and false positive rate are uncertain when a mobile user traverses at a speed less than 20 miles/hour.

3.5.2.2 Migration itinerary based mobile IDS

Hall *et al* (2005) propose a method using public transportation users' mobility profiles to detect intrusions by employing an instance based learning pattern classification technique. By collecting a user's location information from location broadcast of their mobile device, a high level mapping of their location profile can be generated. The comparison process is carried out between a user's current mobile sequence with their profile; if the deviation is larger than the threshold an alert will be raised. The proposed method was evaluated using a simulation method with 50 mobile users who took the public transport service in Los Angeles. All 50 mobile users' location information was inserted into a MySQL database and the simulation process was conducted using the Matlab software package. However, the simulation result was not particularly promising. In addition, according to previous studies, around 50% of all mobile users take the public transport system, i.e. buses or trains (Markoulidakis *et al*, 1995; Wu *et al*, 2001) and so the other 50% of mobile device users who do not use the public transport system cannot be protected by this proposed method.

3.5.3 Comparison of behaviour based mobile IDS

Table 3.3 illustrates the comparison for all the aforementioned behaviour based mobile IDS systems. By studying a user's calling or location activities behaviour based IDS systems can achieve a high detection rate and offer the ability to detect unforeseen attacks. In addition, as the classification and identification procedures are processed by network service providers, it does not require any additional computational power from the mobile device. This has traditionally been critical for mobile devices as they have limited processing power and space compared with traditional desktop computers. Nonetheless, if these behaviour-based systems work together to monitor the mobile user's action (e.g. calling a friend) while knowing where the action is occurring (e.g. at home), the overall system performance could arguably be increased.

Name	Behaviour	Pattern classification model	Detection rate	FAR
Samfat and Molva, 1997	Itinerary	Mathematical formula	82.5%	4%
	Calls	Mathematical formula	80%	3%
Boukerche and Notare, 2002	Calls	RBF neural network model	97.5%	4.2%
ASPECT project	Calls	neural networks	50%	0.02%
Buschkes *et al* 1998	Mobility	Bayes decision rule	87.5%	NA[4]
Sun *et al* 2004	Mobility	High order Markov model	87.5%	15%
Sun *et al* 2006	Mobility	High order Markov model	89%	13%
Hall *et al*, 2005	Itinerary	Instance based learning	50%	50%

Table 3.3: A review of mobile behaviour profiling

3.6 Conclusion

Among the three authentication methods, biometric technique outperforms the other two methods by identifying a person based upon their unique characteristics. The physiological based biometric approaches provide stronger protection: highly unique for individual users and extremely difficult to forge. The behavioural based biometric mechanisms tend to offer more transparent and continuous security throughout a user's normal interaction with a device. To date, many biometric techniques, such as fingerprint recognition and face recognition have been deployed for the purposes of identification and access control.

With more sophisticated mobile devices available, a number of biometric techniques can now be deployed on them to provide continuous and transparent protection, such as behavioural profiling, keystroke analysis and voice verification. Although various investigations have been carried out into these biometric techniques, the majority of them require certain user activities to occur to

[4] Not Available

ensure continuous protection, for instance a user has to press the keyboard to enable keystroke analysis and a voice call has to be made to allow voice verification to be performed. In comparison, the use of behaviour profiling on mobile devices presents an interesting proposal given that every mobile user has to utilise an application/service to perform tasks on their device. As a result, a user's identity could be continuously verified while they are interacting with their mobile devices.

Although little literature was available on behaviour profiling on mobile devices, a significant amount of research work on mobile user's calling and migration behaviour has proved that by using a pattern classification method mobile users can be discriminated by the way they utilise telephony services or the way they carry devices around. However, in practice it can be seen that the mobile network operators can only monitor calling and migration behaviour rather than examining every single mobile service. Therefore, none of the current research in mobile behaviour security approaches provides a comprehensive and continuous protection against device misuse. Hence, a mobile behaviour profiling approach which can offer detection across a wider range of services and connections on the mobile device is needed. The next chapter presents the results of a series of experiments that were conducted to examine the feasibility of utilising behaviour profiling to verify users on mobile devices.

4 Behavioural Profiling on Mobile Devices

4.1 Introduction

It is widely recognised that users of mobile devices utilise mobile services to perform a variety of tasks when interacting with individual applications. Besides factory preinstalled mobile applications, there are more than 1 million mobile applications available for users to choose from, with more applications being added on a daily basis (Apple Inc, 2011; Androlib, 2011). Behaviour profiling has the potential to continuously verify a user in an easy and effective manner: a user is verified based upon which applications they utilise. If the verification of a user was possible while they interact with mobile applications, the verification process could be performed non-intrusively and continuously for the duration of usage.

In order to thoroughly study the possibility of employing behaviour profiling techniques on mobile devices, two types of application behaviour will be examined:

- Intra-standard applications: provide a basic level of information on how a mobile device user utilises the device, such as the name of the application, the time it was accessed and the location at which it was utilised.
- Intra-extended applications: offer richer and more discriminatory information than intra-standard applications do. Apart from providing the basic information, they also offer additional detail on what a user does with them. For example, a telephone call could contain the telephone number being called and the duration of the call.

The literature in Chapter 3 has shown that the existing behavioural based mobile IDS systems can only monitor network-based services (e.g. telephony) through telecommunication service provider's networks. As current mobile devices have the ability to access multiple networks simultaneously, a host based approach must be taken into consideration when investigating a new security mechanism. Little research has been published regarding how behaviour profiling techniques perform within the mobile host environment despite that the mobile application usage represents an overview of how the user interacts with the device (Miettinen *et al*, 2006). Hence, it is critical to identify the effectiveness of utilising the behaviour profiling technique to verify a user's identity via their application usage within the mobile host environment. Although it is proved that the calling behaviour can be utilised to identify mobile users over telecommunication service provider's networks, the calling service's effectiveness towards verifying a user's identity

within the mobile host environment is uncertain as its features have changed slightly, such as the International Mobile Subscriber Identity (IMSI) cannot be utilised anymore. Therefore, a series of experiments examine the aforementioned two types of applications by utilising the behaviour profiling technique within the mobile host environment: intra-standard and intra-extended applications.

4.2 Methodology

4.2.1 Dataset

The experiment employed a publicly available dataset provided by the Massachusetts Institute of Technology (MIT) Reality Mining project rather than create its own (Eagle *et al*, 2009). This is due to the MIT Reality Mining dataset containing a rich amount of information over a long period of time: 106 participants enrolled for the data collection process from September 2004 to June 2005; among these participants, 94 participants' mobile usage activities were successfully logged and the other 12 participants were not. More importantly the MIT Reality Mining databases contain a mixture of mobile user's activities, including the use of intra-standard and intra-extended applications; this meets the need for the behaviour profiling study within the mobile host environment.

By using preinstalled logging software, the MIT Reality Mining dataset was formed by collecting application usage activities from participants' Nokia 6600 mobile phones. An overview of the MIT Reality Mining dataset is presented in Table 4.1. Also, all collected information which may disclose the participants' privacy was anonymised, including the telephone numbers being dialled and texted and the cell tower IDs visited. As shown in Table 4.1, the MIT Reality Mining dataset contains a large amount of information covering several activities: the application usage (intra-standard and intra-extended applications), network usage (Bluetooth activities) and machine usage (when a device was charged). As the location information was collected separately from the applications' usage, the location information was subsequently joined with each application usage record by their date and time stamps.

Activity	Number of logs	Information
Location information	3,308,710	Date, time and cell ID
Application	662,393	Application name, date and time of usage
Bluetooth scanning	1,994,186	Date, time of each scan along and MAC address of individual devices
Charge	11,506	Date and time when the mobile was on charge
Device usage	574,788	Date and time the mobile was in use
On	13,012	Date and time when the phone was turned on
SMS	5,607	Date, time and number of texting
Voice	54,440	Date, time, number of calling and duration

Table 4.1: **The MIT Reality dataset**

For methodological reasons, the experiment utilised a subset of participants whose activities (both intra-standard and intra-extended applications) occurred during the period of 24/10/2004-20/11/2004 to maximise the number of participants. If two users had different start and end dates, the date feature alone would provide the discriminatory information required and skew the results. These activities include intra-standard applications and two intra-extended applications (telephony and text messaging service). Despite several other intra-standard applications also being used by the participants, only a basic level of information was collected by the logging software for them. For instance, all information was gathered for web surfing usage except the web address being visited. As a result, these were treated as intra-standard applications rather than intra-extended applications for this experiment. Also, as the dataset was compiled in 2004, the available choice of mobile applications was limited for mobile users creating a high degree of similarity for intra-standard application usage.

During the 28 days, a total of 105 unique intra-standard applications were used by the selected users. Among these applications, four were removed for this study; the reasons for removal are stated as below:

- Menu: is the gateway to access the majority of applications. In isolation it does not provide much valuable information.
- Context_log: was preinstalled on each participant's phone for the automatic collection of usage information.
- Screensaver: does not provide any information and could be triggered accidently without a mobile user noticing.

- Phone: although it was logged as an 'application', it is not in fact an application merely a button on the mobile phone keypad.

Table 4.2 demonstrates the final dataset for intra-standard applications. Among these 76 participants, 101 applications were utilised for a total of 30,428 times. For instance, user 1 used the camera application in cell_ID 135 at 09:39 am on 28/10/2004.

Number of participants	76
Number of unique applications	101
Number of logs	30,428
Information contained	Application name, date, time and location of usage

Table 4.2: The final dataset on intra-standard applications

All of the 76 participants utilised the telephony service during the chosen period. However, five of them did not have sufficient data for generating a profile and they were excluded from the telephony service study. Therefore, 71 of them were finally employed for the experiment (as shown in Table 4.3). Between these users, 2,317 unique anonymised telephone numbers were dialled with a total of 13,599 times. For example, user 3 called the anonymised telephone number 591 in cell 361 at 04:32 pm on 05/11/2004 and the conversation lasted for 16 minutes and 32 seconds.

Number of participants	71
Number of unique dialled telephone numbers	2,317
Number of logs	13,599
Information contained	Anonymised telephone number, date, time, duration and location of usage

Table 4.3: The final dataset on telephony service

Among the 76 participants, 49 users utilised the text messaging service during the chosen period. Nevertheless, once again 27 of them did not have sufficient data for generating a profile and they were not selected for the text messaging service study. As a result, only 22 of them were included in this study and their text message usage is summarized in Table 4.4. There were 258 unique telephone numbers being texted accumulated 1,381 times. For instance, user 20 sent a text message to the anonymised telephone number 192 in cell 925 at 11:21 am on 17/11/2004.

Number of participants	22
Number of unique telephone numbers	258
Number of logs	1,381
Information contained	Anonymised telephone number, date, time and location of texting

Table 4.4: The final dataset on text messaging service

4.2.2 Procedure

The experiment employed the mathematical software package MATLAB developed by MathWorks as the investigation platform. The literature on behaviour profiling in Chapter 3 identified classification methods that performed well and they fall into two categories: statistical and neural network approaches. Based upon the "no free lunch" theorems, there is no single classification method that can solve all given problems (Wolpert and Macready, 1997), three classification methods were chosen from these categories to identify an optimal classifier to solve the behaviour profiling problem within the mobile host environment: the Radial Basis Function Neural Network, the Feed-Forward Multi-layered Perceptron Neural Network and a Rule-based approach.

To investigate individual classifiers, a number of scripts were created to perform various tasks, such as data extraction and classifier selection. Several of these scripts were commonly employed for each classification approach and they are:

- Data Extraction function: extracts users' behaviour records from the MIT Reality Mining dataset into the MATLAB programming environment and return each record entry for each individual user respectively.
- Feature Selection function: based upon individual behaviour, various features (e.g. telephone number) are selected from the records.
- Normalisation function: normalises selected data into the range of 0-1. Sola and Sevilla (1997) suggested that input data normalisation is a critical procedure prior to a training process as well normalised input data can obtain good results and also accelerate significantly calculations.
- Dataset Split function: splits a selected dataset into two halves; the first half is used for building a profile and training a classifier; the other half is used to validate the performance of a classifier.
- Classifier Selection function: chooses a classifier and sets up the parameters of the classifier.

- Evaluation function: calculates the FAR, FRR and EER to evaluate the performance of a selected classifier.

The calling sequence for each function is illustrated in Figure 4.1: users' behaviour information flows from one function to another via the directional arrows. Figure 4.2 demonstrates three classifiers within the Classifier Selection function. Any mathematical solutions can be chosen for mathematical formulae classifiers such as a Rule-based classifier. The Multilayered Perceptron Network and RBF neural network were chosen for the neural network based classifiers because of their well-known abilities in the pattern classification domain.

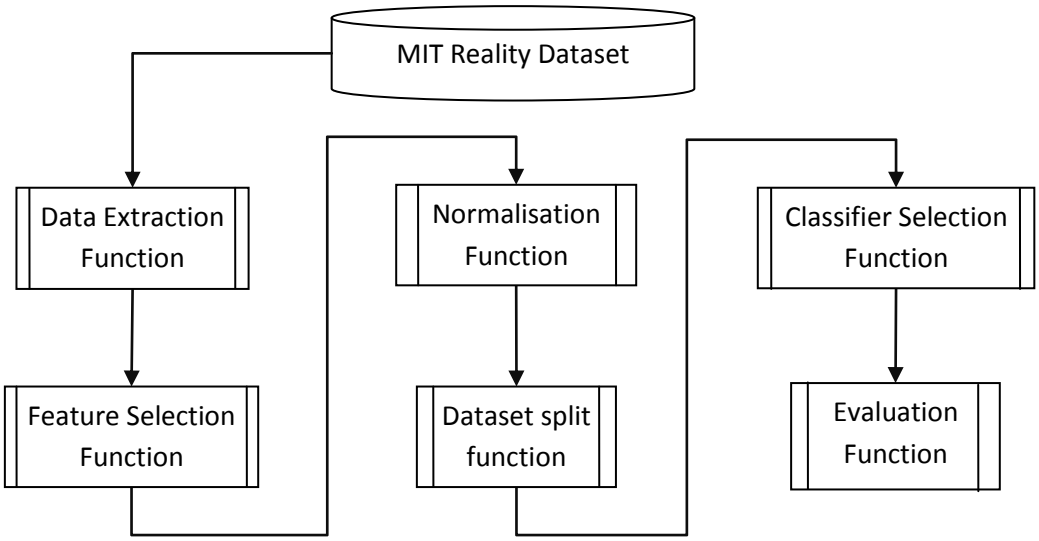


Figure 4.1: Behaviour profiling system functions flow diagram

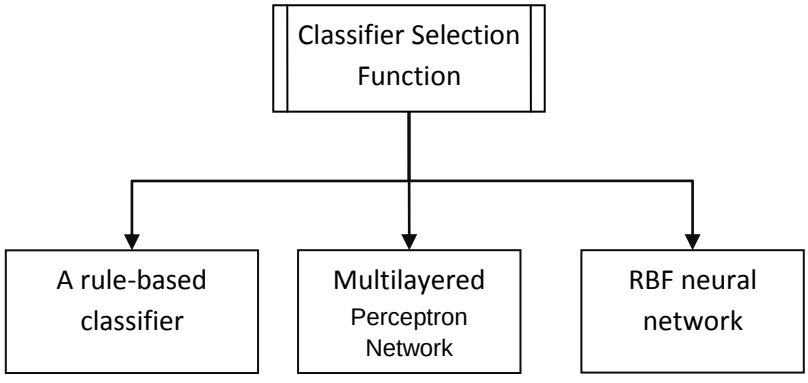


Figure 4.2: The three classifiers being employed

4.3 The results

Three sets of experimental studies were formed: two preliminaries and one complete. The first preliminary study utilised a descriptive statistical approach to analyse the raw information presented by the datasets. It is well-known that the statistical method has the ability to determine potential positive applications' features for forming unique patterns to discriminate individual users (Jain *et al*, 2000). Also, the selection of effective features is a critical process in pattern classification as the system performance is closely related to the features and large number of features will increase the complexity and the size of the classifier (Fu *et al*, 1970). The second set preliminary study was conducted to fulfil two purposes: to identify the most optimal classifier for solving the behaviour profiling issue in the mobile host environment and to determine positive behaviour profiling features through experiments. The complete study was proposed to examine the feasibility of employing behaviour profiling on mobile devices through application activities (intra-standard applications, intra-extended applications and multi-instance (combination of intra-standard and intra-extended) applications).

4.3.1 A Descriptive statistics study

It is well known that the descriptive statistical method is capable of describing the main features of a dataset in quantitative manners. In order to examine potential positive features for behaviour profiling on intra-standard and intra-extended applications, two descriptive statistical studies were conducted. For the intra-standard applications, the following features were available and were examined: the name, time and location of an application being accessed. For the intra-extended applications, the following features were available and were analysed: the name, time and location of an application being utilised, plus the extra information the intra application offers.

4.3.1.1 Descriptive statistics on intra-standard applications

Figure 4.3 demonstrates that the participants utilised various applications during the chosen period. It is possible to identify users based upon the application name alone if no two users activated the same application. For instance, user 4 is identifiable among all users by uniquely utilising application 30 during the chosen period. However, as also presented in Figure 4.3, the participants did share a number of commonly used applications: the phonebook, call logs and camera were used by all 76 users; while the message centre application was used by 75 users (all apart from user 56). In addition, they cumulatively represented 72% of the total intra-standard applications usage (as shown in Figure 4.4). Therefore, it would be difficult to discriminate users solely based upon the applications they utilised over a chosen period. However, if the participants

did utilise a variety of applications, they could be easily discriminated from each other using the application name feature.

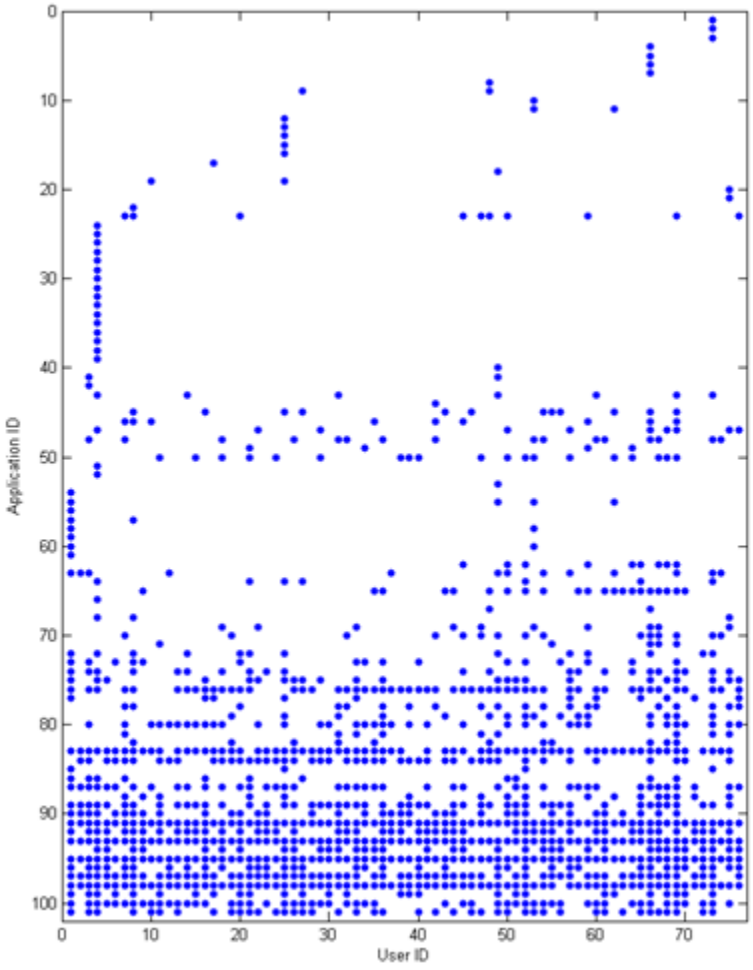


Figure 4.3: Users with their applications

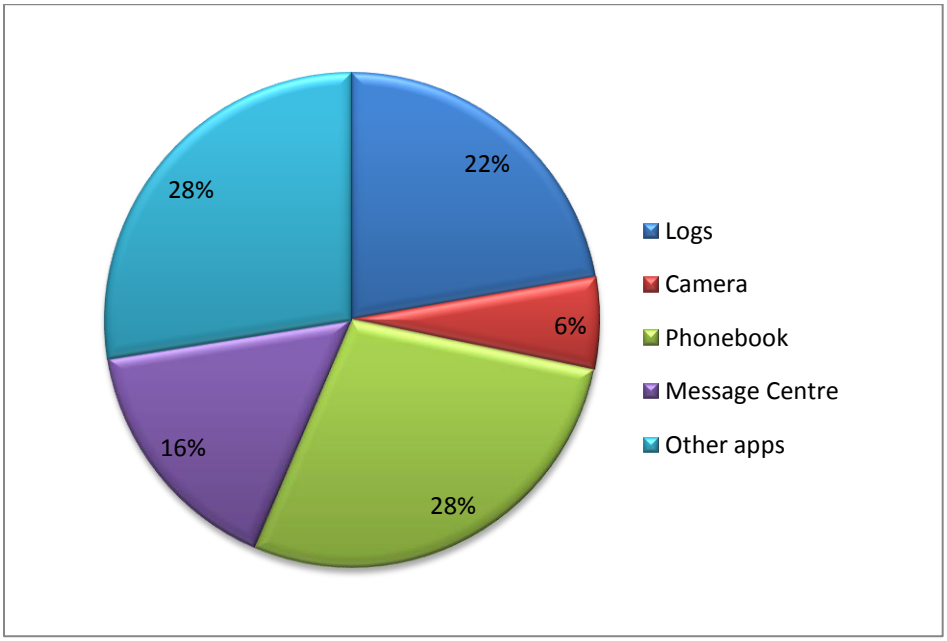


Figure 4.4: Overview of intra-standard application usage

Apart from the application name feature, two other features were also examined: the location feature and the time feature. Four applications were chosen for the experiment as the majority of the participants utilised them and these applications were the camera, logs, message centre and phonebook.

When a mobile application is utilised, the location details can be gathered via one of the following methods: coordinates (i.e. longitude, latitude and altitude) through a GPS service, mobile cell IDs through a telecommunication operator's network, wireless network IDs through a Wi-Fi connection, and Bluetooth Media Access Control (MAC) addresses via a Bluetooth connection. The level of precision provided by these methods varies: a set of coordinates can be utilised to pinpoint a user within 1 square metre while a wireless network ID can cover up to 10,000 square metres. The application location information in the dataset is presented in the form of cell IDs. Depending upon the location of a cell tower, its coverage varies: larger in rural areas and smaller in urban districts. Nonetheless, these will generate a level of similarity in location usage for those who regularly work or study on the same site. As the MIT Reality Mining data was collected from a mixture of 106 MIT students and staff, similar location usage could occur during the data collection process.

Figure 4.5 depicts all locations being utilised by all users for their camera application usage during the 4 week chosen period. Among these users, user 6, user 46 and user 63 did not share any cells with any other users. On average, all users only shared one cell between each other. As a result,

the majority of the users could be discriminated by using the cell ID feature despite them all utilising the same application. In the worst scenario, user 22 and user 40 shared the most number of cells (as shown in Table 4.5). Although they shared 5 cells, their usage on these locations were somewhat different: user 22 spent most of their usage in cell 20, logging 23 times, while user 40 recorded only 3 times in the same location (i.e. cell 20). Therefore, a level of dissimilarity still exists between their usage within these 5 cells. In addition, as the similarity usage represented 41.5% and 39.1% of their total usage respectively, the rest of their location usage of the camera application could still be separated.

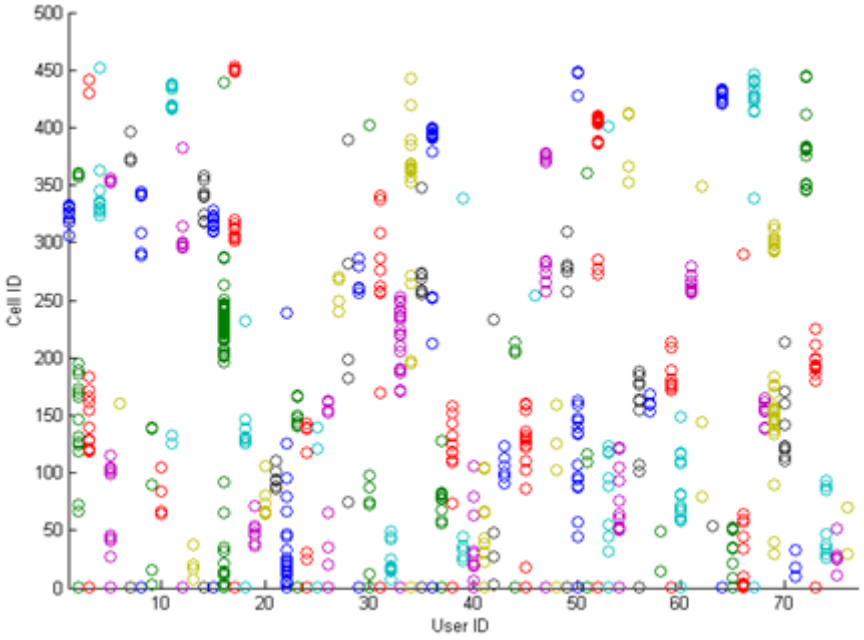


Figure 4.5: The location comparison for all users' camera application usage

	Cell ID	1	6	19	20	79	Proportion of total usage
Usage	User 22	1	2	2	23	1	41.5% (65)
	User 40	1	2	2	3	1	39.1% (23)

Table 4.5: The cell comparison for User 22 and User 40's camera application usage

The location for all users' logs application usage is depicted in Figure 4.6. On average, each user only shared 2 cells with another user. For the best case, user 1, user 67 and user 46 only shared 1 cell with some users. As the majority of users utilised their logs application in different locations, they could be discriminated between each other despite them all using the logs application. Further investigation was carried out on those who had similar location usage for the logs application. For instance, user 43 and user 50 shared 10 cells during the chosen period (as shown in Table 4.6). For the same locations they used, no distinct usage difference is shown apart from

user 43 utilising cell 12 significantly higher than user 50 did. This certainly would generate some obstacles to separating them on those usages. Nonetheless, as the amount of similar usage only represented 23.5% of user 50's total usage, the other 76.5% of its usage could still be identified by employing cell IDs alone. In comparison, it would be difficult to identify user 43's activities with user 50's as the similarity usages represent almost 58% of their total usage.

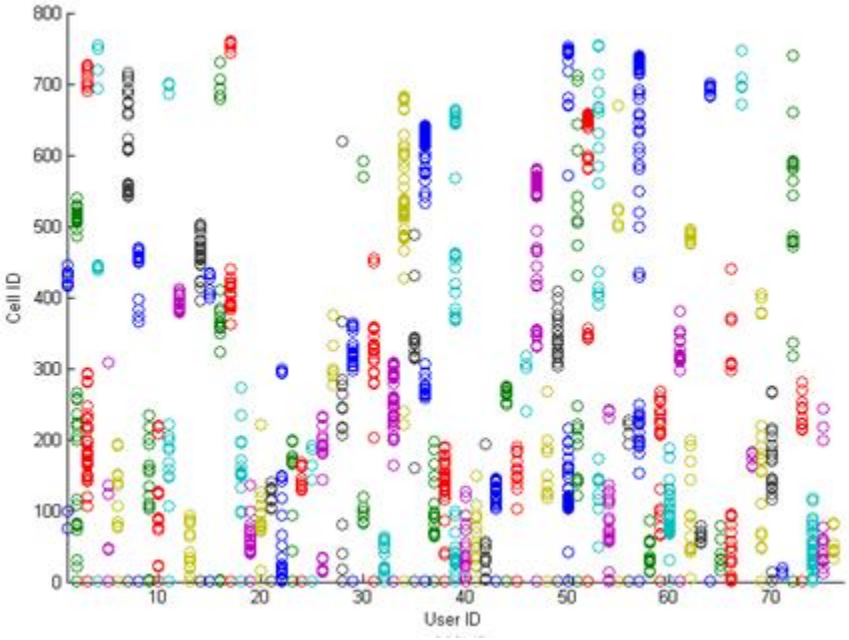


Figure 4.6: The location comparison for all users' logs application usage

	Cell ID	1	103	106	110	112	118	119	121	130	133	Proportion of total usage
Usage	User 43	7	2	5	1	13	28	1	2	2	2	57.8% (109)
	User 50	9	1	1	3	2	33	1	1	1	1	23.5% (226)

Table 4.6: The cell comparison for User 43 and User 50's logs application usage

Figure 4.7 demonstrates the comparison on the location for the users' message centre application usage. In general, each user only shared 1 cell with another user during the chosen period. For the best scenario, user 71 did not share any cells with any other users. As a result, user 17 is identifiable among all users by using the cell ID feature alone. In the worst scenario, user 59 shared 9 cells with user 73 and details are depicted in Table 4.7. Despite them both utilising 9 identical locations, their usage on these cell IDs was somewhat different: user 59 spent the majority of their usage in cell 1 and cell 76 while user 73 utilised cell 41 as its major usage location. In addition, as the similar usage only represent 24.8% and 22.1% of their total usage for user 59 and user 73 respectively, a large proportion of their location usages could still be separated using the cell ID feature.

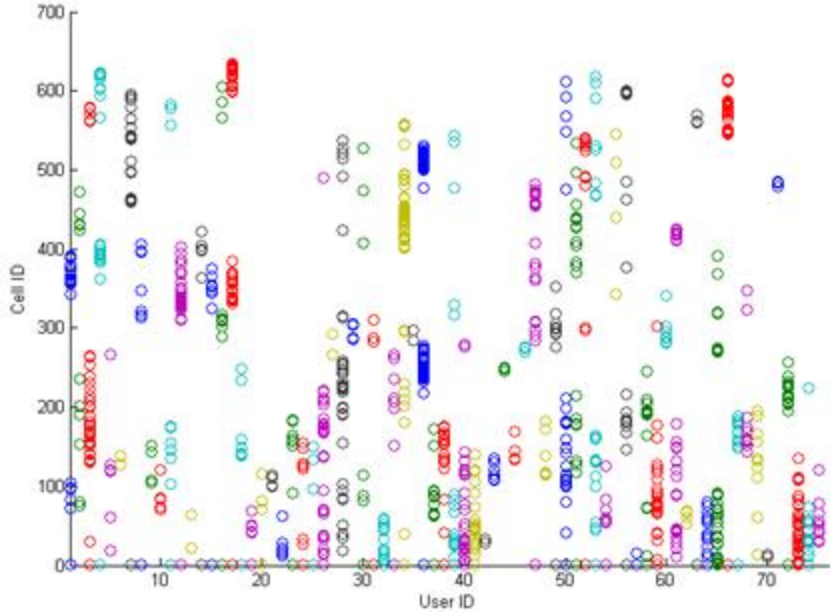


Figure 4.7: The location comparison for all users' message centre application usage

	Cell IDs	1	31	40	41	66	75	76	77	110	Proportion of total usage
Usage	User 59	11	1	1	1	2	1	8	1	3	24.8% (117)
	User 73	6	9	2	33	7	3	6	4	1	22.1% (321)

Table 4.7: The cell comparison for User 59 and User 73's message centre application usage

Figure 4.8 demonstrates the location comparison for all users' phonebook application usage during the chosen period. Among these users, user 71 did not share any cells with any other users. As a result, it could be identified based upon the location feature alone. On average, each user only shared 2 cells with another user. For the worst case, user 41 and user 66 shared 10 cells (as shown in Table 4.8) for location usage of their phonebook application. Although the usage on these 10 cells represent 70.8% and 62.5% of their total usage, they utilised these cells very differently: user 41 spent the majority of location usage in cells 1, 77 and 18; while user 66 utilised cell 49 most of their time. As a result, the majority of their usage could still be separated despite them sharing 10 cells during the chosen period.

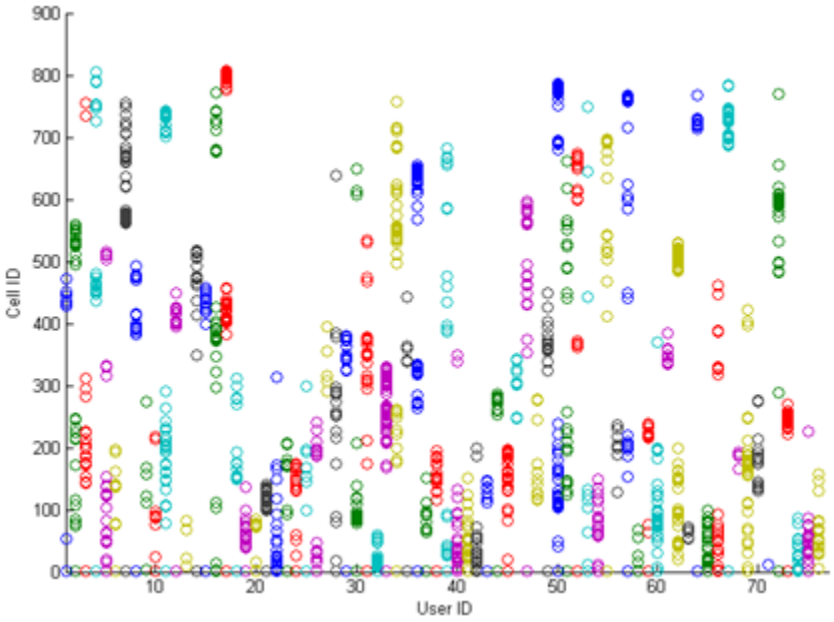


Figure 4.8: The location comparison for all users' phonebook application usage

	Cell IDs	1	2	28	29	35	36	37	49	76	77	Proportion of total usage
Usage	User 41	191	1	1	3	1	1	18	7	2	49	70.8% (387)
	User 66	4	8	1	1	3	2	2	31	2	1	62.5% (88)

Table 4.8: The Cell comparison for User 41 and User 66's phonebook application usage

As demonstrated above, in general the location of an application being used provides positive information for discriminating mobile users. Although a number of users did share large numbers of cells during the chosen period, the data presented in Tables 4.5 – 4.8 have shown that the usage on each individual cell amongst different users can still vary significantly. As a result, a level of discrimination could still be obtained even for users who had been in similar locations when their devices were utilised. This could be potentially used for identifying misuse by friends and colleagues.

The time of using an application can be logged when the application is started. For instance, a user makes a phone call (application) at 07:05:19 AM (time stamp). The time of accessing the camera, logs, message centre and phonebook from all users are depicted in Figure 4.9, Figure 4.10, Figure 4.11 and Figure 4.12 respectively. In general, no clear patterns are shown between individual users' access times on these four applications. However, the figures do highlight several usage differences between groups of users. For example, user 34 and user 36 used the logs application most of the time. On the other hand, little usage is shown by user 5 and user 71 for the same application. Another example, the time at which user 40 and user 75 utilised the phonebook

covered most of the time spectrum. In comparison, little usage was observed for user 46 and user 68 for the same application. As a result, it is difficult to separate one heavy (light) usage user with another heavy (light) usage user due to the underlying similarity. Nonetheless, their usage patterns could be utilised in the following manner: for the heavy usage users, if their devices have not been used for a period of time, this could be a sign of intrusion and vice versa.

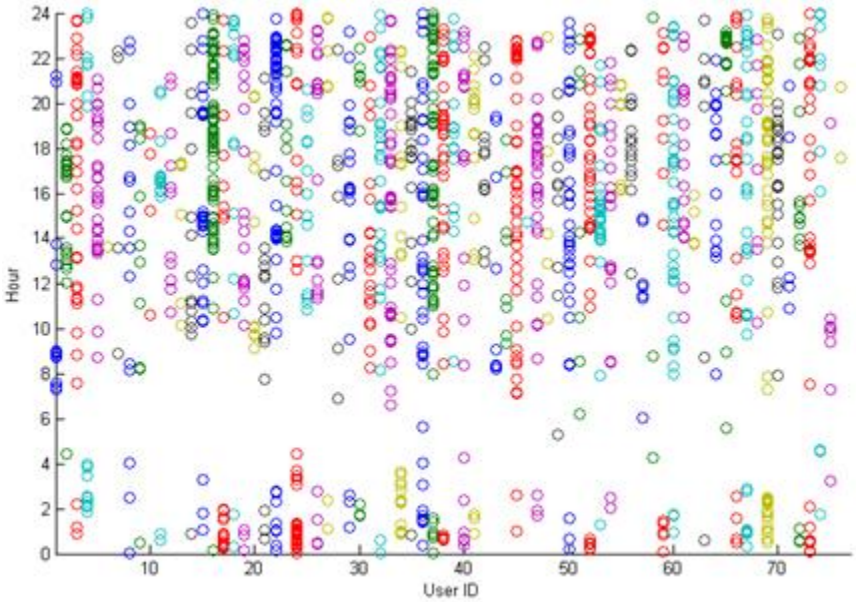


Figure 4.9: The time of accessing comparison for users' camera application usage

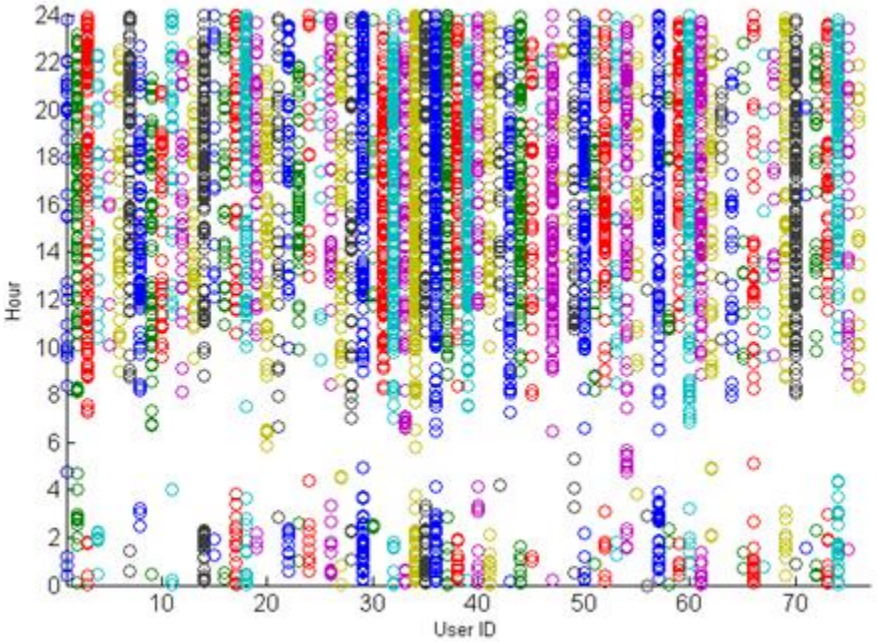


Figure 4.10: The time of accessing comparison for users' logs application usage

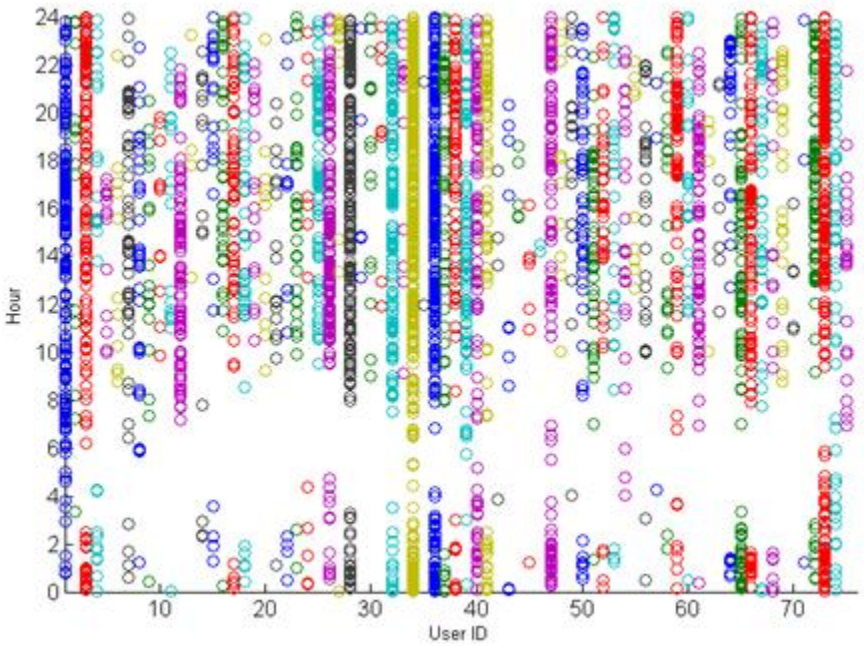


Figure 4.11: The time of accessing comparison for users' message centre application usage

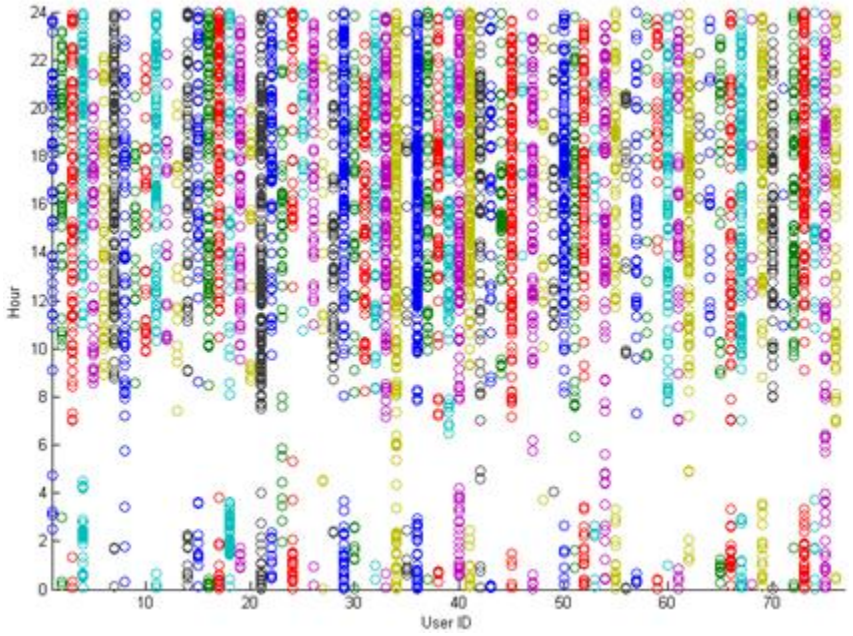


Figure 4.12: The time of accessing comparison for users' phonebook application usage

4.3.1.2 Descriptive statistics on intra-extended applications

4.3.1.2.1 Telephony

For the 71 telephony users, a number of their telephony features were extracted from the dataset: the location, time and duration of calling, plus the telephone number being dialled.

The comparison for all these 71 users' telephony location usage is depicted in Figure 4.13. Among these users, user 59 only shared 1 cell with a few other users despite it is difficult to visualise in Figure 4.13 due to the large cell IDs' range in a relative small graph. On average, each individual user shared 1 cell ID with another user. As a result, most of the telephony users could be identified from each other based upon the location feature. Nonetheless, the identification process could be difficult for some users due to their high level of usage similarities. For instance, among all users, user 20 and user 36 had a maximum of 12 cells in common. As demonstrated in Table 4.9, although they have been to the same locations, their frequency of appearance in these cells were markedly different: user 20 spent most of their usage in cells 113, 129 and 131, while user 36 spent majority of their usage in cell 129. As a result, the majority of their similar activities could still be separated based upon their historical usage in these locations.

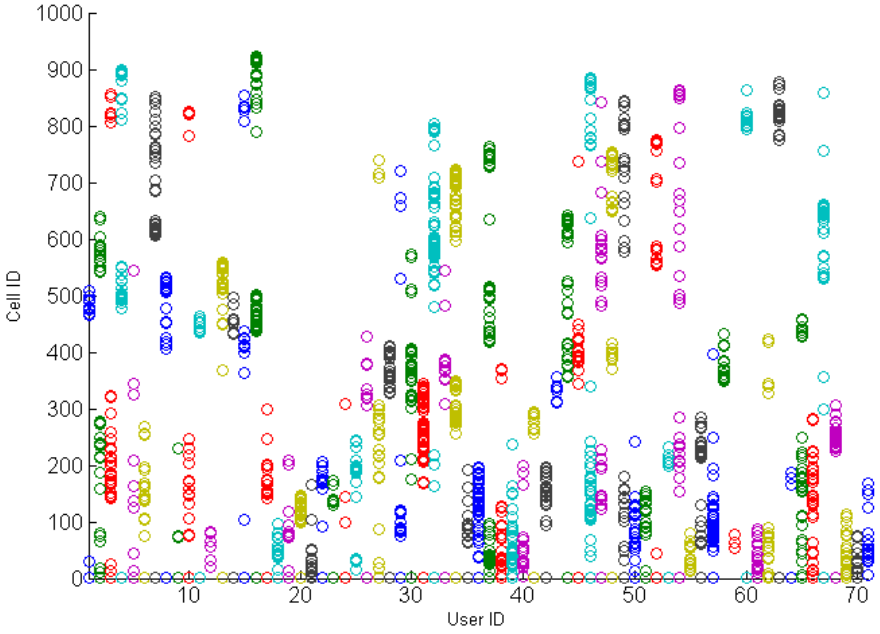


Figure 4.13: Users telephony location usage comparison

	Cell IDs	1	113	114	118	129	130	131	132	142	143	145	146	Proportion of total usage
Usage	User 20	4	51	14	6	21	2	20	2	1	1	2	6	41.8% (311)
	User 36	12	3	6	1	107	1	2	1	2	3	1	9	46.7% (317)

Table 4.9: Telephony location usage comparison for user 20 and user 36

Figure 4.14 depicts all 71 users' telephone number usage during the chosen period. Among these users, user 26, user 33 and user 59 did not share any telephone number with any other users. On average, each user only shared one telephone number with another user. Hence, based upon the

telephone number feature alone, the majority of the mobile device users could be discriminated from each other. However, some users did share a number of telephone numbers during the chosen period, which might increase the difficulty for the classification process. One of the reasons behind this could be that these users may have friends and/or colleagues in common and that is why they called the same telephone numbers. This could be used to evaluate the performance of a classifier in the scenario where friends misuse each other's devices. For instance, user 34 and user 63 shared a maximum of 9 telephone numbers, as outlined in Table 4.10. Although these two users had similar usage on these 9 telephone numbers, distinct usage patterns still exist between them: user 34 used the anonymised telephone number 1237 heavily when compared with other telephone numbers. While user 63 employed the anonymised telephone number 1247 and anonymised telephone number 1271 most often. Therefore, they could still be discriminated between each other to a certain extent based upon their historical usages on these telephone numbers.

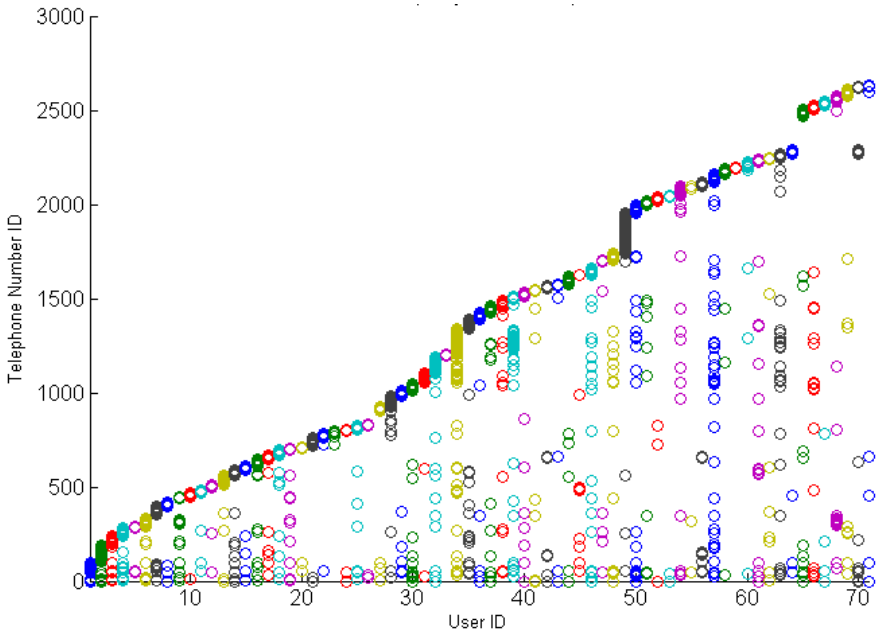


Figure 4.14: Users telephony telephone number usage comparison

	Telephone number	779	1071	1139	1237	1247	1269	1271	1287	1329	Proportion of total usage
Usage	User 34	1	2	4	88	1	10	2	17	24	19.2% (775)
	User 63	5	1	8	2	11	7	15	4	1	31.8% (170)

Table 4.10: Telephone number usage comparison for user 20 and user 36

The comparison for all these 71 users' telephony time of calling is presented in Figure 4.15. The pattern presented by the time of calling feature of the telephony was similar to those demonstrated by the four applications' time of usage in previous section. It is difficult to identify individual users by using the time of calling feature in isolation. However, how a person uses the telephone application can be obtained based upon their historical usage: when the telephone application is most likely to be used and when it is unlikely to be used. For instance, user 68 frequently used the telephony application during the period from 2pm to 7am. If the telephony application is used outside this time frame, it could be a sign of misuse on user 68's device. If less usage is observed for the telephony application inside the aforementioned time frame, it also could be a sign of abnormal activity (e.g. user 68's device may be lost).

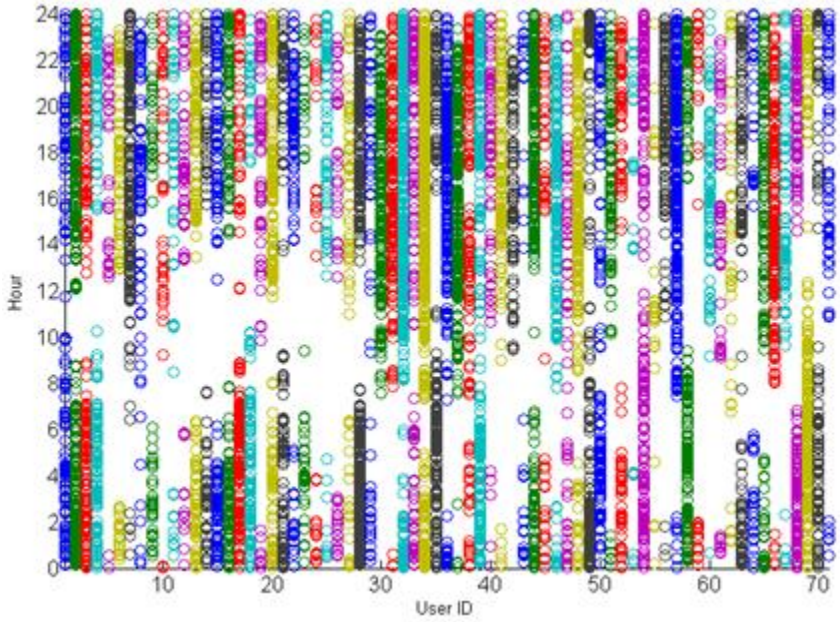


Figure 4.15: Users telephony time of calling comparison

All users' telephony durations of calling are depicted in Figure 4.16. In general, no clear difference is shown by the figure apart from the majority of calls lasting less than 300 seconds. Indeed, as demonstrated in Figure 4.17, for all 13,719 calls, 95.7% of them lasted less than 10 and 50% of them lasted less than 30 seconds. There are many factors which may affect the duration of a telephone call, such as the relationship between calling parties, how often they communicate, what topic they discuss and even the surrounding environment. Despite the variety of reasons behind how long a call may last, with the observed percentages it is clear that it could be difficult to discriminate users from each other by using the duration of calling alone.

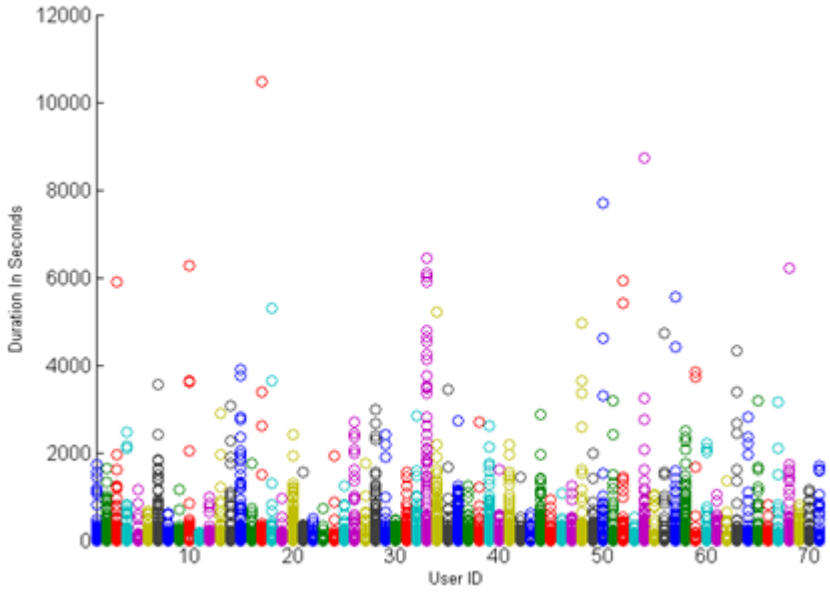


Figure 4.16: Users telephony duration of calling comparison

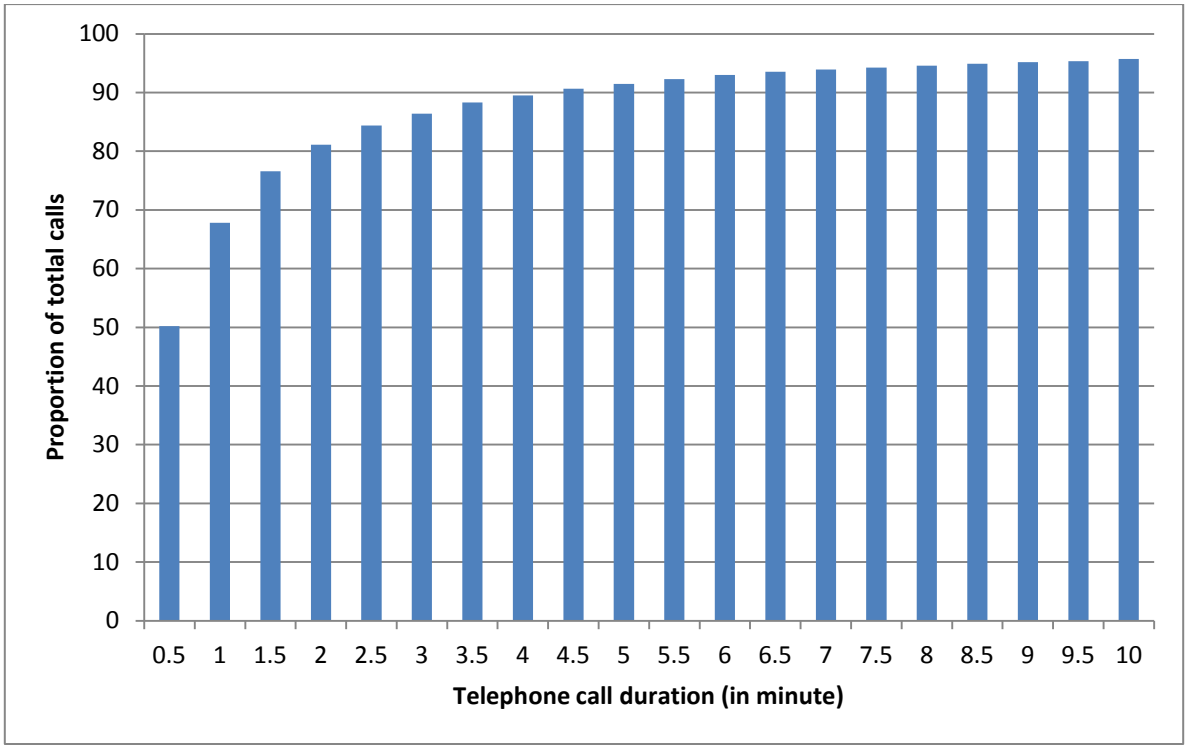


Figure 4.17: A cumulative distribution for all users' telephone call duration

4.3.1.2.2 Text messaging

For the 22 users' who utilised the text message service, the following features were available and extracted from the text message dataset: the telephone number being texted, and the location and time of the text being sent.

Figure 4.18 depicts all the users' text message location usage during the chosen period. The usage of text messaging was much less compared with other aforementioned applications'. For the best case, user 13 did not share any cells with any other users. On average, each user only shared one cell with another user. Therefore, in general the majority of these 22 users could be discriminated from each other based upon the location feature. Nonetheless, it may be difficult to identify several users due to their similar location usage. For instance, user 3 and user 12 shared a maximum 4 cells together as shown in Table 4.11. It is hard to separate their usage for these four locations because they did not exhibit significant usage difference. This similarity of usage could have little impact on user 3 as the usage only represents 11.1% of their total text messaging usage. In comparison, it could be more difficult to differentiate user 12's activities from user 3's due to the large proportion of similar usage.

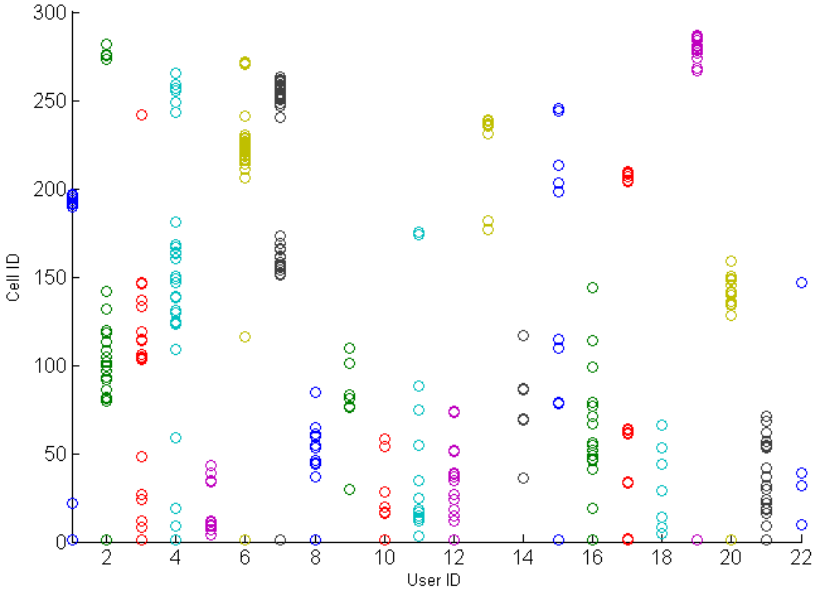


Figure 4.18: Location usage comparison of users' text message

	Cell ID	1	12	24	27	Proportion of total usage
Usage	User 3	2	2	3	2	11.1%(81)
	User 12	4	1	1	5	40.7%(27)

Table 4.11: The location usage comparison for user 3's and user 12's text messaging service

All these 22 users' text message telephone numbers usage is shown in Figure 4.19. The figure indicates that significant usage difference existed on the texted telephone numbers between each user. Indeed, a total of nine users did not share any telephone numbers with any other user. By using the number of texting feature alone, these nine users can easily be discriminated. For the worse case, user 6 and user 12 only shared 2 telephone numbers with each other and their usage

quantity for these two locations is shown in Table 4.12. As both users did not have significant usage in these two locations, it is difficult to separate their usage of these locations from their historical usage. Moreover, as the similar usage only represents 2.2% of user 6's total usage, user 6 can still be easily identified. In comparison, the verification process may not be so easy for user 12 as the common usage represented 22.2% of their total usage.

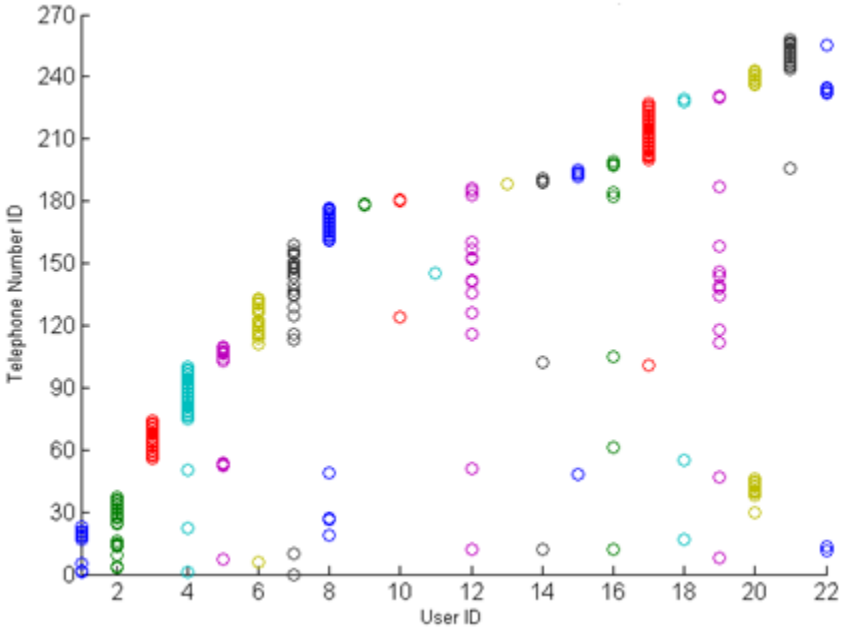


Figure 4.19: Users text message telephone number usage comparison

	Telephone number	116	131	Proportion of total usage
Usage	User 6	1	1	2.2% (91)
	User 12	3	3	22.2% (27)

Table 4.12: Text message telephone number usage comparison for user 6 and user 12

Figure 4.20 outlines all 22 users' text message sending time during the chosen period. In general, based upon the time of the sending feature alone, it could be difficult to identify individual users from each other. However, this feature has the potential to be used for generating patterns on how a user utilises the text messaging service: when the service is more likely to be used and when it is not. For instance, apart from the period of from 4 am to 8 am, the chance of user 7 sending a text message is much higher. As a result, any message sent by user 7 outside the aforementioned timeframe could be considered as normal. In comparison, if a message is sent at 5 am, the chance that user 7's device is being misused could be significantly higher.

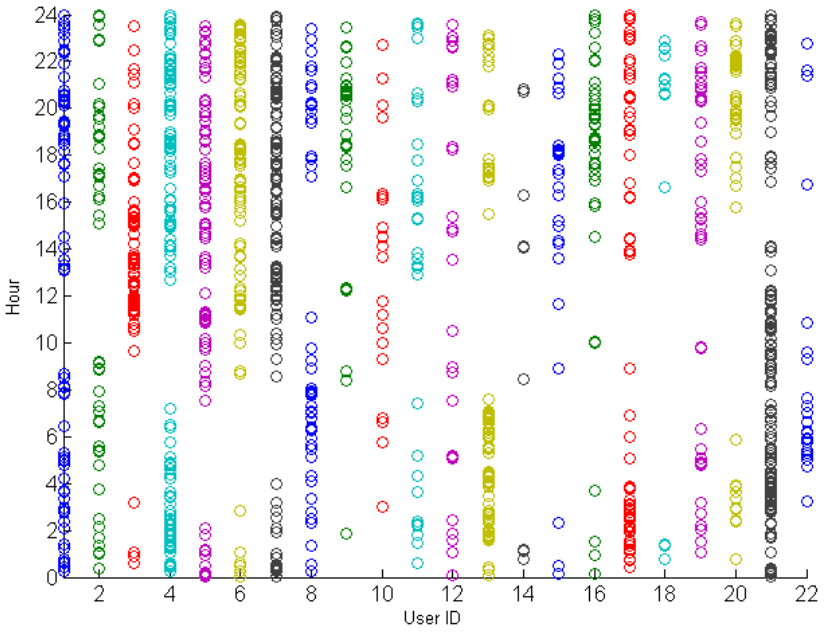


Figure 4.20: Users text message time of sending comparison

From the above analysis, it demonstrates that the chosen experimental dataset contains a huge amount of users' mobile device activities represented by their applications usage. Although it could be seen that the majority of the users utilised their devices differently (especially for intra-extended applications), a level of similarity was also observed for some users in the applications they used and also where and when they used those applications. Moreover, a number of features have the potential to be used for discriminating mobile users. For the intra-standard applications, users could be separated via individual applications' names if they did not utilise the same applications. For those who utilised common applications, the utilisation location of an application could contribute information towards to successful individuation. By knowing where an application was used, the majority of the users could be discriminated. This indicates that the location of usage could be a positive feature for classifying mobile users. For the intra-extended applications: both telephony and text messaging services, apart from the location of usage, the telephone calling/texting feature could also be very useful in distinguishing mobile users.

In comparison, by using the application activation time feature alone, it could be difficult to discriminate users from each other. This may be caused by there only being 24 hours in a day: the longer the chosen period (i.e. more days), the higher the chance that two users will activate the same application at the same time or within a similar time frame. However, these applications' activation time figures do show certain patterns of when the devices are more likely to be used and in which periods they are less likely to be used. By using this information, certain abnormal

activities could be detected by a security system, such as during the periods a device is likely to be active and when there is no activity on the device and vice versa.

4.3.2 A preliminary study on telephony activity

The descriptive statistical study identified several features which may provide positive information for a classification process. Hence, a preliminary study was conducted to explore these features' effectiveness towards behaviour profiling using a more scientific approach. As the full dataset contains large amount of information: more than 30,000 logs for intra-standard applications alone, it will require a huge amount of computational power and time to identity the usefulness of each application feature by employing the whole dataset. As a result, the preliminary study utilised a sub-dataset which was extracted from the main telephony service dataset. The sub-dataset contained a total of 3,836 call logs from 20 randomly selected users. In this way, the identification process on the impact that a feature of an application plays for a classification result can be carried out in a more efficient and less time consuming manner. As mentioned earlier in this chapter, there is no single classification method that can solve all given problems, three generic pattern classification approaches were employed for the behaviour profiling technique: RBF neural network, FF MLP neural network and a rule-based method. Therefore, the optimal classifier should have the best performance and require the least computational power. For the actual experiment, each user's data was divided into two halves: the first half was used to generate a profile and the other half was used to evaluate the classifiers' performance. The results for the preliminary study are presented in the following sections.

4.3.2.1 Radial Basis Function Networks

An RBF neural network has been one of most popular pattern classification methods used in the Artificial Intelligence (AI) field. By default, it has three network configurations: number of neurons, the performance goal and spread. For this preliminary study, only the number of neurons parameter was configured while the other network configurations remained at the default settings. Table 4.13 demonstrates the best selected RBF neural network configurations with several combinations of telephony features as the inputs. The full set of experimental results is presented in Appendix B. Table 4.13 demonstrates the average results for the FAR, FRR and EER from these 20 chosen users. In general, the results show that by using an RBF neural network, the telephony application can be used to discriminate users within the mobile host environment. By employing the dialled telephone number and the location of calling features as the inputs with 75 neurons, the RBF network achieved the best performance with an EER of 10.5% (also shown in Figure 4.21).

By adding the time of calling and/or the duration of a call features as additional RBF neural network inputs in addition to the telephone number and location features, the users can still be discriminated from each other although the overall performance decreased rapidly. Therefore, both the time and duration of calling features cannot be considered as positive features to classify mobile users in this case.

Features	Features Employed	Number of neurons	FAR	FRR	EER
Telephone number (1), location (2), duration (3), time (4)	1, 2, 3, 4	75	13.9%	15.8%	14.9%
	1, 2, 4	100	13.7%	15.3%	14.5%
	1, 2, 3	50	13%	13%	13%
	1, 2	75	10.7%	10.2%	10.5%

Table 4.13: The best RBF network configurations with various features

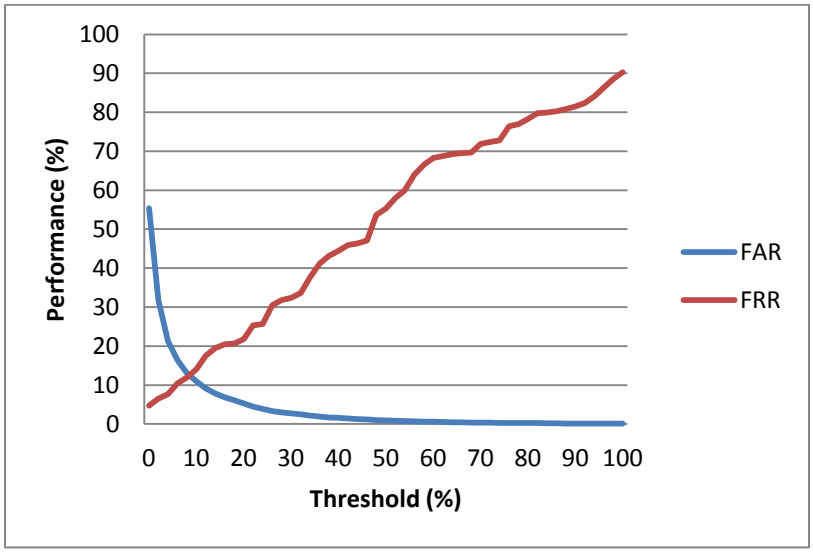


Figure 4.21: FAR-FRR plot for the RBF network performance (Inputs: telephone number and location with 75 neurons)

4.3.2.2 Feed-Forward Multi-Layered Perceptron Network

The Feed-Forward Multi-Layered Perceptron (FF MLP) Network is another widely employed AI technique utilised in the pattern classification domain for many years. With more network configuration variables available, the FF MLP neural network is a more complex classifier compared with the RBF neural network. Therefore, to solve the same problem, the FF MLP neural network should require more computational power than the RBF neural network does. Apart from modifying the number of neurons parameter, other configuration of the FF MLP neural network remained as default. Table 4.14 demonstrates the best FF MLP network configurations with various combinations of calling features as the inputs of the classifier. The full set of experimental results is presented in Appendix B. In general, these mobile users can be classified using the FF

MLP neural network although the performance was not as good as employing the RBF neural network. As shown in Table 4.14, by using the dialled telephone number and the location of calling as the inputs and applying 150 neurons for the FF LMP neural network, the classifier obtained its best performance producing an EER of 17.5% (also shown in Figure 4.22). However, with more features (adding the time and/or duration of calling) as the inputs, the performance of the classifier tended to decline. Therefore, the results demonstrate that both the time and duration of calling did not provide a positive contribution towards classification.

Features	Features Employed	Number of neurons	FAR	FRR	EER
Telephone number (1) , location (2), duration (3), time (4)	1, 2, 3, 4	125	11.9%	30.6%	21.3%
	1, 2, 4	100	11.5%	29.7%	20.6%
	1, 2, 3	150	10.5%	40%	24.7%
	1, 2	150	14.9%	20.1%	17.5%

Table 4.14: The best FF MLP network configurations with various features

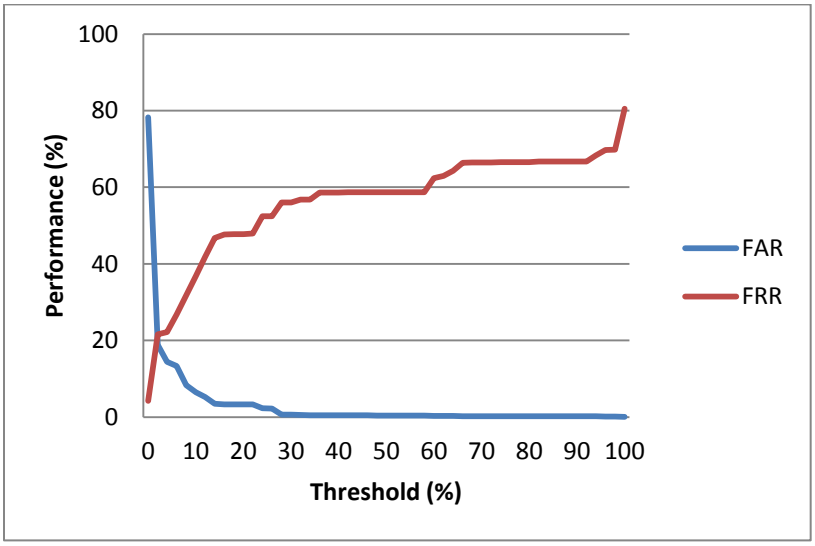


Figure 4.22: FAR-FRR plot for the FF MLP network performance (Inputs: telephone number and location with 150 neurons)

4.3.2.3 A rule-based approach

The basis for this approach was derived from the descriptive statistics produced when analysing the data and the large variances observed. A dynamic approach therefore seemed sensible to cope with the changing nature of the profile. Based on the premise that the historical profile can be used to predict the probability of a current event, the rule-based approach illustrated in Equation 1 was devised. The approach also includes a weighting factor (W_i) to allow more discriminative features to have a greater contribution within the resulting score than less discriminative features do. Moreover, the approach also provides a mechanism to ensure all outputs are bounded between 0 and 1 to assist in defining an appropriate threshold.

Equation 1: Alarm if: $1-\frac{\sum_{i=1}^{N}\left(\frac{\text{Occurance of Feature}_{ix}}{\sum_{x=1}^{M}\text{Occurance of Feature}_{ix}}\times W_i\right)}{N}\geq$threshold

Where:

i=The features of one chosen application (e.g. dialled number for telephony application)

x=The value of $Feature_i$ (e.g. office telephone number and home telephone number)

M=Total number of values for $Feature_i$

N=Total number of features

W_i=The weighting factor associated with $Feature_i$ ($0< W_i \leq 1$)

Threshold= A predefined value according to each individual user

For example, a user uses an application with only the location feature (N=1). During the past 4 weeks, the user utilised that application in location 1, 2 and 3 (M=3) for 50, 40 and 10 times respectively. According to the above approach, the probability when the user utilises that application in location 1 next time is 50% (50/(50+40+10)). A value obtained by 1-the probability will be compared with a pre-defined threshold and a decision will be made accordingly. When application has more than 1 feature, the average probability will be compared with the threshold.

By employing the above approach, a number of experimental tests on the 20 users' telephony activities were conducted. Apart from the weighting factor for each feature being set to 1, other parameters within the formula were chosen appropriately according to the selected telephony features. The results from the experiment are presented in Table 4.15. By using the dialled telephone number and location of calling features, the rule-based approach obtained a best result EER of 11% (also shown by Figure 4.23). By adding other calling features, such as time of calling and/or duration of calling, the performance of the classifier decreased significantly. This indicates that neither the time of calling nor the duration of calling is a positive feature for the telephony service for this particular dataset.

Features	Features Employed	FAR	FRR	EER
Telephone number (1) , location (2), duration (3), time (4)	1, 2, 3, 4	18.3%	21.9%	20.1%
	1, 2, 4	8.1%	16.7%	12.4%
	1, 2, 3	17.8%	21.7%	19.7%
	1, 2	7.1%	14.8%	11%

Table 4.15: Experimental results by employing the rule-based approach

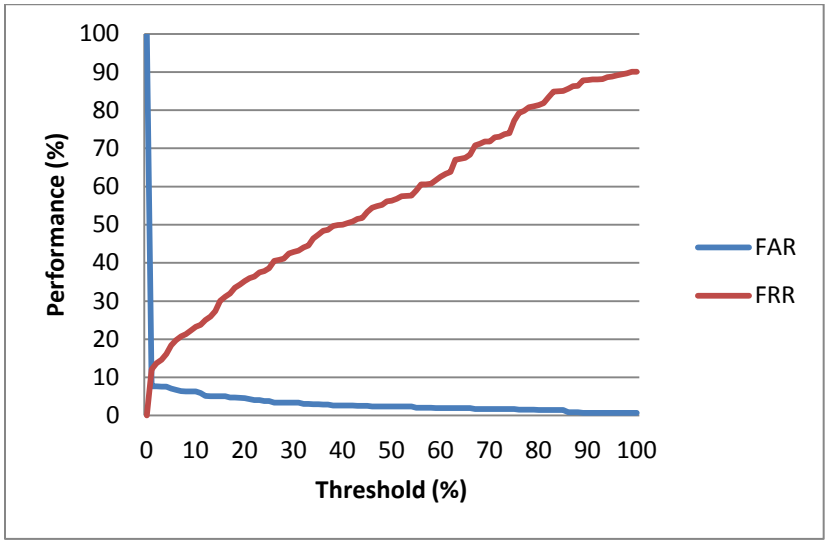


Figure 4.23: FAR-FRR plot for the performance of the rule-based approach

4.3.2.4 Discussion on the preliminary study

Based upon the above three sets of results, the preliminary study demonstrates that mobile users can be discriminated by using the telephony service within the mobile host environment with a good level of performance. Also, the preliminary study identified the usefulness of each application feature towards to the classification result as illustrated in Table 4.16. Both the dialled telephone number and location of calling features proved to be positive calling features for discriminating the mobile users by each of the three classifiers. In comparison, by adding the time of calling and/or duration of calling features as additional inputs the classifiers' performance got worse. This indicates that neither feature can be considered as contributing positive information towards the classification process. In addition, the previous statistical analysis also suggested that: both the dialled telephone number and location of calling features could contain strong discriminatory information to separate mobile users, while both the time and duration of calling features could contain less significant user classification information.

Feature	Contribution to the classification result
Telephone number	Positive
Location of calling	Positive
Duration of calling	Negative
Time of calling	Negative

Table 4.16: Individual application features towards to the classification result

Among the three chosen classifiers, the FF MLP neural network achieved the lowest performance despite more computational power (in terms of number of neurons) being employed. In addition, several other issues for the FF MLP neural network were observed from the experiment. For

instance, the FF MLP neural network stopped early during the training phase resulting in undesired output. In comparison to the FF MLP neural network, both the RBF neural network and the rule-based approach achieved much better performances. Although the RBF neural network had a slightly higher performance (0.5% in terms of EER) than the rule-based approach, it also consumed a significantly greater amount of computational power than the rule-based approach did. This might be feasible if the classification process is undertaken in a desktop computer environment. Nonetheless, the rule-based approach is still favoured because of its simplicity and fast decision making. Also, as the classification process itself will be performed within the mobile host environment, an average mobile device will struggle to provide sufficient computing power to house an RBF neural network based classifier. Even if the mobile device could offer the required computing power; it is highly likely that it would take a longer time for the RBF neural network based classifier to process the same amount of data than it would for the rule-based approach. Furthermore, as the RBF neural network is considered as a black box approach, any implementer would have less control to the classifier apart from the three available network configurations; in comparison, the rule-based approach is more simple, dynamic, configurable and adaptive, such as each mobile application can be applied with its own weighting towards the classification process. As a result, the rule-based approach was employed as the classifier with which to progress the next step of the research.

The three FAR-FRR plots (Figure 4.21, Figure 4.22 and Figure 4.23) also demonstrate some insights for the preliminary study. As the majority of the FAR rates were smaller than 10% for all threshold settings, it indicates that a significant difference exists between mobile users in their telephony service usage. Therefore, this information will assist a classifier to discriminate mobile device users from each other more easily. In comparison, a significant proportion of the FRR rates were bigger than 10% for all threshold settings. Such a result suggests that a large variance may exist across each individual mobile user's telephony usage, which is a common problem all behavioural based biometric systems have to anticipate. Nonetheless, the situation could be improved by employing a dynamic profiling technique for mobile users to minimise the impact caused by their irregular mobile usage. In addition, a smoothing function which utilises a number of application entries as one large event will also be considered to cope with the relevant high false rejection rate issue for the legitimate mobile users.

4.3.3 Behaviour profiling on mobile applications

Based upon the findings from the descriptive statistics and preliminary studies, a complete experiment was undertaken on mobile users' applications usage using the rule-based approach with the combination of the application name, location usage and specific features (i.e. telephone numbers). Two types of profile techniques were employed: static and dynamic. For static profiling, each individual dataset was divided into two halves: the first half was used for building the profile and the other half was used to test the performance of a classifier. For dynamic profiling, the profile contains 7/10/14 days of each user's most recent activities and is updated on a daily basis. As a result, a classification result is made based upon the most recent user's activities (within 7/10/14 days) rather than some usage that occurred four months ago and is therefore not at all relevant to current user behaviour. The evaluation process was carried out on the same sub-dataset as the static one. A smoothing function was also introduced to cope with the mobile users' inconsistent usage behaviour observed in the preliminary study. The smoothing function treats a number of successive applications as one event; as a result, a decision is made based upon the combined event rather than each single application activity. The user's acceptance of the behaviour profiling technique could also be increased: an alarm will not be raised when a user utilises a new application on their device for the first time but when a number of consecutive new behaviours have occurred. The following sections contain a complete behaviour profiling experimental study on a mobile user's application usage: intra-standard, intra-extended and multi-instance applications.

4.3.3.1 Intra-standard applications profiling

For intra-standard applications, the experiment employed the intra-standard applications dataset (as described in Table 4.2). The following features were extracted from the dataset: application name, date of initiation and location of usage. The date of initiation feature was used for generating the profile and evaluating data for the static and dynamic profiles. The profile of an application contains its location usage during the profile period. By using the rule-based classifier, a complete set of experimental results (in the form of EER) for users' intra-standard application usage is presented in Table 4.17. The best performance (EER 13.5%) was obtained by utilising a 14 day dynamic profile with the smoothing function of 6 application entries. In comparison, by employing a 7 day dynamic profile with the smoothing function of one application entry, the classifier obtained the worst performance with an EER of 24%.

		Number of application entries					
		1	2	3	4	5	6
Profile technique	Static 14 days	21.1%	17.4%	16.3%	14.9%	14.2%	13.6%
	Dynamic 14 days	21.1%	17.3%	16.0%	14.5%	14.0%	13.5%
	Dynamic 10 days	22.1%	17.8%	16.2%	14.6%	14.4%	13.7%
	Dynamic 7 days	24.0%	19.4%	17.6%	15.9%	15.3%	14.4%

Table 4.17: Experimental results for intra-standard applications

Figure 4.24 and Figure 4.25 illustrate the worst and best configuration FAR-FRR plots for the 14 day dynamic profile on intra-standard applications. By utilising more application entries in the smoothing function, the performance improved significantly in the terms of a lower FRR and EER. In comparison, the average FAR increased slightly which means an imposter receives a greater opportunity to gain entry into the system.

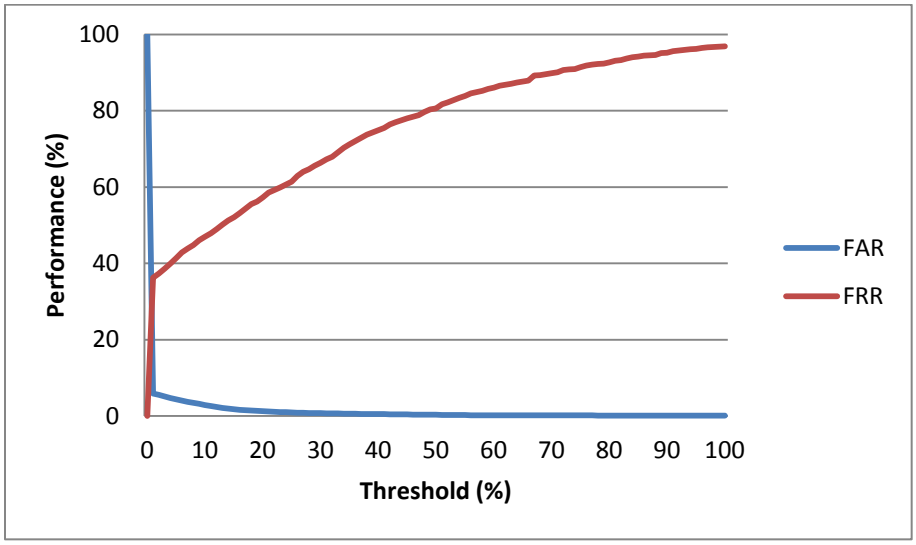


Figure 4.24: FAR-FRR plot for intra-standard applications with the dynamic 14 day profile with 1 application entry

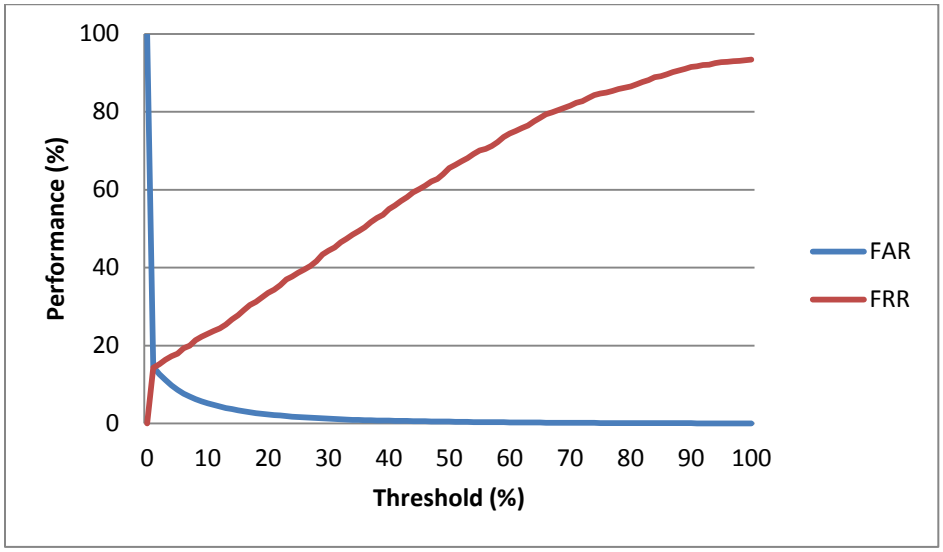


Figure 4.25: FAR-FRR plot for intra-standard applications with the dynamic 14 day profile with 6 application entries

Table 4.18 demonstrates the selected experimental results for the best classifier configuration of intra-standard applications. The top 3 and bottom 3 users' EERs represent the best and worst performance respectively. Also, by using the same configuration, 84.2% of all users had an EER less than 20%.

User_ID	EER
71	0%
46	0%
12	0.5%
66	37.5%
2	39.3%
68	51.6%

Table 4.18: Selected users' performance for intra-standard applications, employing the best classifier configurations

4.3.3.2 Intra-extended applications

4.3.3.2.1 Telephone call

The telephone call experiment employed the telephony dataset (described in Table 4.3). The following features were extracted from the dataset for each log: the telephone number, date of calling and location of calling. The date of calling was utilised for generating the profile and evaluation data according to the profile configuration. For each user's telephone profile, it contains the telephone number and location of usage during the profile covering period. By employing the rule-based classifier with the selected features, a complete set of experiment results for users' telephone call usage is shown in Table 4.19. The best experimental result for the

users' telephony activity is an EER of 5.4% and it was achieved by using the 14 day dynamic profile technique with the smoothing function of 6 telephone call entries. In contrast, the worst performance result (EER of 10.4%) is almost twice as high as the best one and it was obtained via the 7 day dynamic profile with the smoothing function of just one telephone call entry.

		Number of telephone call entries					
		1	2	3	4	5	6
Profile technique	Static 14 days	9.6%	9.1%	7.9%	7.2%	4.3%	6.4%
	Dynamic 14 days	8.8%	8.1%	6.4%	6.4%	6.3%	5.4%
	Dynamic 10 days	9.6%	8.6%	8.1%	7.2%	6.9%	6.0%
	Dynamic 7 days	10.4%	8.8%	8.5%	7.3%	7.0%	6.2%

Table 4.19: Experimental results for the telephone call application

The FAR-FRR plots for the worst and best configurations, employing the 14 day dynamic profile on users' telephony activities are illustrated in Figure 4.26 and Figure 4.27 respectively. These two figures demonstrate that significant improvement occurred for the overall performance by considering 6 telephone call entries as one user's activity.

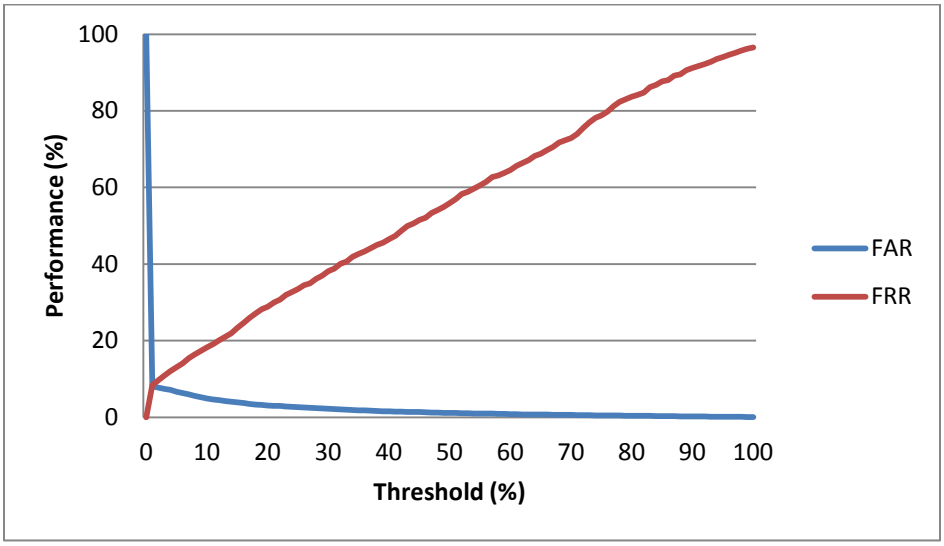


Figure 4.26: FAR-FRR plot for the telephone call application with the dynamic 14 day profile with 1 telephone call entry

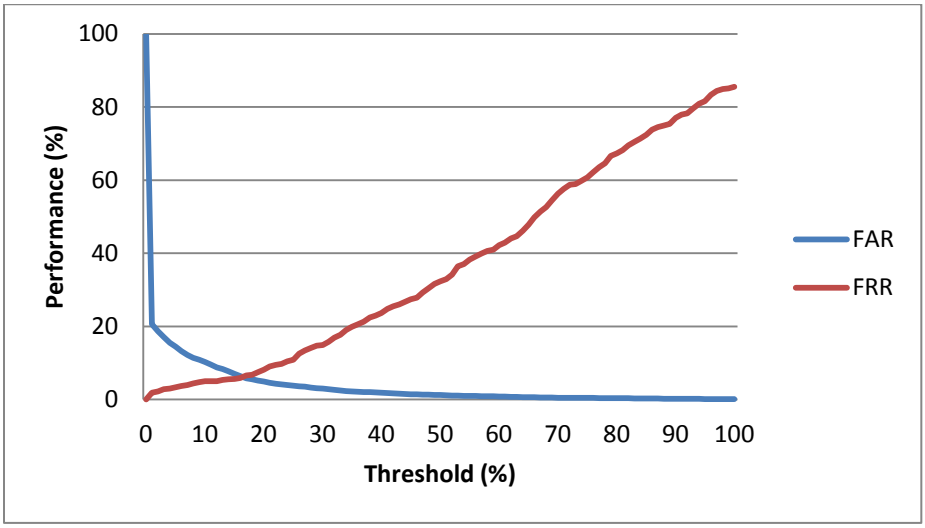


Figure 4.27: FAR-FRR plot for the telephone call application with the dynamic 14 day profile with 6 telephone call entries

A selection of experimental results from the configuration of the best classifier for the telephone call application is presented in Table 4.20. The best and worst performances for the top 3 and bottom 3 users have been selected accordingly. Also, 81.7% of users have an EER less than 10% with the same configuration.

User_ID	EER
23	0%
43	0%
61	0%
64	20.6%
50	23.1%
8	39.5%

Table 4.20: Selected users' performance for the telephone call application by employing the best classifier configuration

4.3.3.2.2 Text messaging

The text messaging experiment utilised the dataset described in Table 4.4. For each text log entry, the following features were extracted from the dataset: texted telephone number, date and location of texting. The date feature was employed for creating the profile and evaluation data according to the individual profiling technique. For each user's text message profile, it contains all usages for the texted telephone numbers and locations of texting during the profile period. Due to several participants texting a limited number of messages over the chosen 28 day period, a maximum of 3 log entries were utilised for the smoothing function. By employing the rule-based classifier and a combination of telephone number and location features, the complete result for user's text messaging application usage is shown in Table 4.21. The best result is an EER of 2.2%

and it was acquired by the classifier utilising the 14 day dynamic profile with a smoothing function of 3 text message entries. Similar to the worst performance result obtained for the telephony service, the lowest performance for the text messaging application is an EER of 10.7% and it was obtained utilising a 7 day dynamic profile and smoothing function of just one text message entry.

		Number of text message entries		
		1	2	3
Profile technique	Static 14 days	7.0%	4.3%	3.6%
	Dynamic 14 days	5.7%	2.6%	2.2%
	Dynamic 10 days	8.3%	4.1%	3.7%
	Dynamic 7 days	10.7%	5.7%	3.8%

Table 4.21: Experimental results for the text messaging application

Figure 4.28 and Figure 4.29 demonstrates the FAR-FRR plots for the users' text message worst and best performance with the 14 day dynamic profile configuration. By utilising more text messages within the smoothing function, the system performance improved significantly.

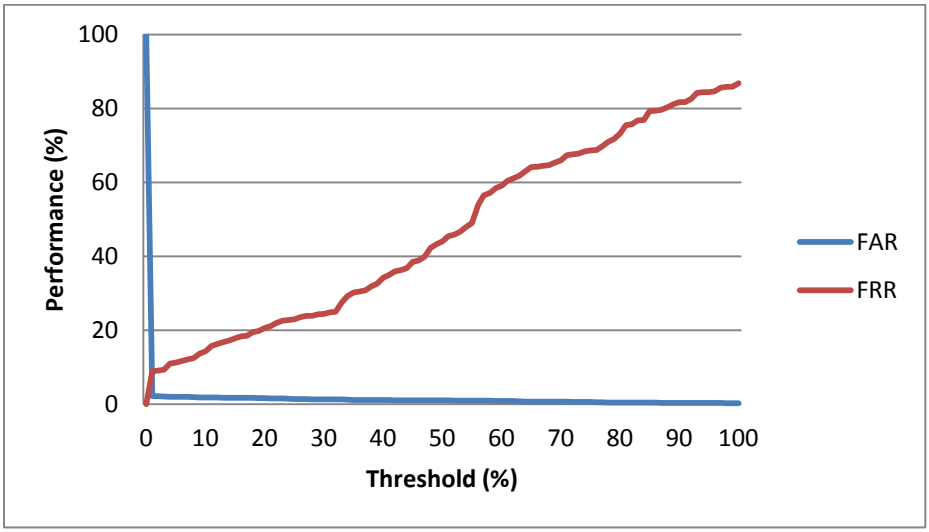


Figure 4.28: FAR-FRR plot for the text messaging application with the dynamic 14 day profile with 1 text message entry

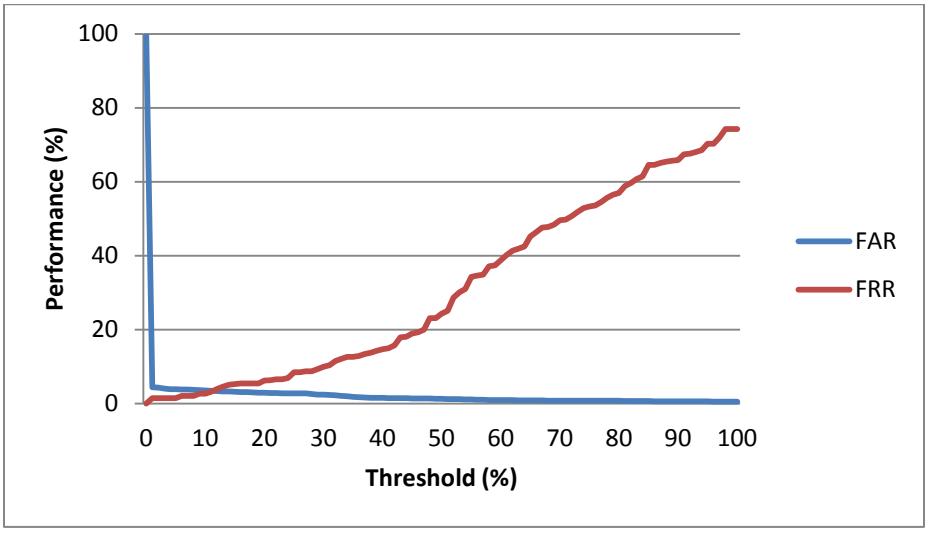


Figure 4.29: FAR-FRR plot for the text messaging application with the dynamic 14 day profile with 3 text message entries

Table 4.22 demonstrate a group of users' performance for the best classifier configuration of the text messaging application. The top 3 and bottom 3 users' EERs represent the best and worst performance respectively. Also, by utilising the same classifier configuration, 95.5% of all users exhibit an EER less than 10%.

User_ID	EER
13	0%
14	0%
18	0.2%
4	5.3%
2	8.4%
17	13.1%

Table 4.22: Selected users' performance for the text messaging application with the dynamic 14 day profile and 3 log entries

4.3.3.3 Multi-instance applications

In daily life, mobile users utilise their applications in a chronological order. For instance, a user switches off the clock alarm (intra-standard application) at 6:05 AM, then visits a number of news websites (intra-extended application) at 6:20 AM, at 7:10 AM, they make several phone calls (intra-extended application) and start listening to music (intra-standard application) at 7:36 AM. As a result, the multi-instance applications can continuously present an image of what a user does on the whole, while either the intra-standard or intra-extended applications could only partially provide information on a user's activity. Also, more importantly, it is envisaged the new security mechanism would verify the user's identity based upon the multi-instance method. Hence, an

experiment was created to examine the performance of the multi-instance applications technique for constantly monitoring every single activity to identify abnormal mobile usage.

For the multi-instance applications experiment, all 76 users' applications activities which were employed separately in the intra-standard and intra-extended applications experiments were utilised. For each user, their intra-standard and intra-extended applications were joined together by using the time and day stamp in a chronological order. Also, features were selected according to their application categories. In total, 30,428 intra-standard applications logs and 15,101 intra-extended applications logs were employed for this set of experiments. By employing the rule-based approach, the experimental results for users' multi-instance applications activities are demonstrated in Table 4.23. By utilising the dynamic profiling technique with 10 days of profiling data and a smoothing function with 6 log entries, the best result of EER 10% was obtained. In comparison, the worst result of EER 19% was acquired by employing the dynamic profiling technique with 7 day of profiling data and the smoothing function with 1 log entry.

		Number of log entries					
		1	2	3	4	5	6
Profile technique	Static 14 days	16.9%	13.6%	12.7%	12%	10.9%	11%
	Dynamic 7 days	19 %	15.2%	13.1%	12.4%	11.3%	10.5%
	Dynamic 10 days	17.4%	13.7%	12.3%	11.6%	10.6%	9.8%
	Dynamic 14 days	16.5%	13.5%	12.1%	11.6%	10.5%	10.1%

Table 4.23: Experimental results for multi-instance applications

Figure 4.30 and Figure 4.31 illustrate the worst and best configuration FAR-FRR plots for the 10 day dynamic profile on multi-instance applications. By utilising more application entries in the smoothing function, the performance improved significantly in the terms of a lower FRR and EER. In comparison, the average FAR increased slightly which means an imposter receives a greater opportunity to gain entry into the system.

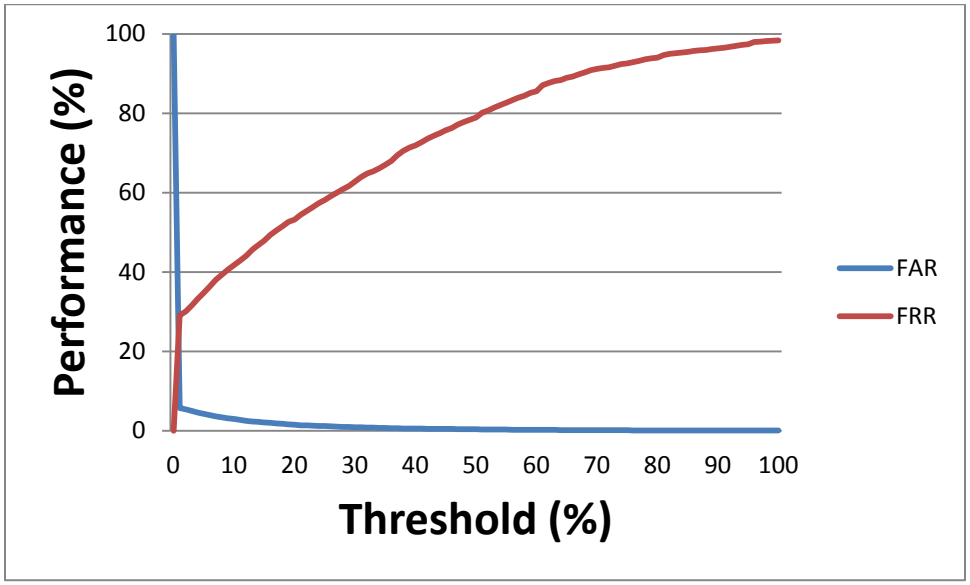


Figure 4.30: FAR-FRR plot for multi-instance applications with the dynamic 10 day profile with 1 application entry

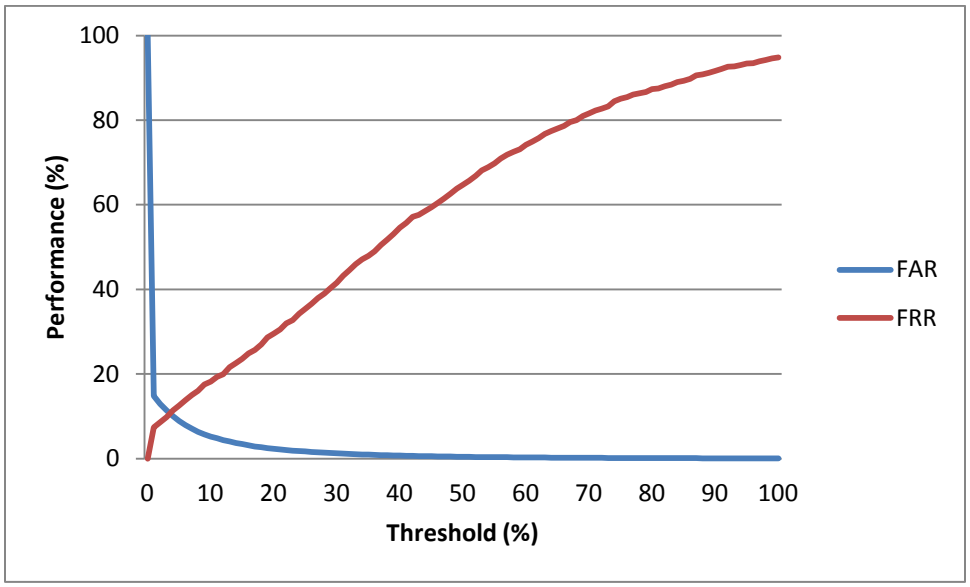


Figure 4.31: FAR-FRR plot for multi-instance applications with the dynamic 10 day profile with 6 application entries

Table 4.24 illustrates a group of users' performance for the best configuration of the multi-instance applications experiment. The top 3 and bottom 3 users' EERs present the best and worst performance respectively. Also, 55.3% of all users have an EER smaller than 10% and 80.2% of all users have an EER lower than 15%.

User_ID	Performance
46	0%
71	0%
63	0%
68	20.2%
69	25.4%
8	28.8%

Table 4.24: Selected users' performance for multi-instance applications with the dynamic 10 day profile and 6 log entries

4.4 Discussion

The application name and location of usage are valuable features that can provide sufficient discriminatory information to identify mobile users. However, whilst this might identify many misuse scenarios, it would not necessarily identify all cases of misuse – particular those where a colleague might briefly misuse a device because the location information is likely to fall within the same profile as the authorised user. So care is required in interpreting these results. The intra-extended application approach should also help to specifically identify this type of misuse.

In general, the dynamic profiling technique achieved a slightly better performance than the static profiling technique did. This is reasonable as a dynamic profile contains a user's most recent activities; hence it achieves more accurate detection. Furthermore, with a longer profile period, the performance is also improved. Hence, an increased number of days (e.g. 18/22 days) of user activities as a profile should be examined to find the optimum solution. Nonetheless, literature suggests users do change their usage pattern over a long period of time. Flurry (2009) suggests that users only keep 67% of new applications beyond a 30 day period. Moreover, storage and processing issues should also be taken into consideration with larger profile sizes. While a smoothing function treated more application entries as one incident, the performance also improved accordingly. The smoothing function reduces the impact any single event might have and seeks to take a more holistic approach to monitoring for misuse; this will provide a user-friendly environment as fewer rejections occur and more convenient when a user changes their usage behaviour. The disadvantage of this approach is that it takes a longer time for the system to make a decision; hence, an intruder could have more opportunities to abuse a system and a degree of abuse might be missed by the security control.

Limitations in the dataset are also likely to have created certain difficulties. As the dataset was collected in 2004, the number of mobile applications available for users to choose from was limited; this resulted in a large similarity of intra-standard applications usage between mobile

users and difficulty for any classification method. In contrast, in January 2012, there were more than 1 million applications available in the mobile applications market. As mobile users have a greater available choice their intra-standard applications usage would arguably differ more. Therefore, it would be easier to discriminate mobile users through their intra-standard applications usage.

As shown by Table 4.19, the performance of the telephony application is very good – more than twice that of the intra-standard applications profiling. This reinforces the hypothesis that knowing both the application and what the user does with it, improves the chance of identifying individual users significantly. Moreover, mobile users had a far larger set of telephone contacts (the numbers they can dial) compared with the number of applications they had, making the classification process easier because there are more identifiable data points from which to discriminate. In comparison with other biometric authentication techniques as described in Chapter 3, the telephone experiment is within that category of performance.

As presented in Table 4.21, the results from the text messaging application were even better than those achieved by the telephone call application, albeit with a smaller dataset. This may be caused by people only sending text messages to very close contacts. Although only 30% of the participants used the text messaging application in 2004, the situation has changed considerably: for the UK alone, the volume of text messaging traffic has increased by 290% since 2004 (Ofcom, 2010). This indicates that the text messaging based authentication method could serve a good proportion of the mobile user population.

As demonstrated in Table 4.23, the experimental results for the multi-instance application are in between the results from the intra-standard and intra-extended applications; this is within the expectation as the experiment utilised the combination of both types of applications. Also, it is envisaged that the larger the proportion of intra-extended applications users have, the better the performance of a system. As a result, the process of differentiating whether an application belongs to the intra-extended category and extracting their features accordingly is mission-critical for a behaviour profiling system.

As illustrated in Table 4.25, the performance of the behaviour profiling technique is within the expectation of the overall behavioural biometric category within the mobile device environment. In addition, although it is more difficult to profile certain users, more than 80% of all users' performance was within the bounds of a behaviour-based biometrics. Dynamic-based profiling

techniques provide the opportunity to develop a more meaningful profile of user activities. This does however raise issues with regards to template ageing and ensuring the samples utilised in creating the template are all legitimate, which will need to be addressed. Furthermore, this approach employed a light weight rule-based approach which saves a significant amount of processing power and storage space; this is essential for handheld mobile devices as they are limited in these two areas.

Behavioural techniques	Performance (EER)
Behaviour Profiling	10%
Gait recognition (Derawi *et al*, 2010)	20.1%
Keystroke analysis (Clarke and Furnell, 2006)	13%
Handwriting recognition (Clark and Mekala, 2007)	1%
Voice verification (Woo *et al*, 2006)	7.8%

Table 4.25: The behavioural techniques performance within the mobile device environment

4.5 Conclusion

The results prove that mobile device users can be discriminated from each other based upon their application usage by a number of experimental studies. By using the descriptive statistics method, two major findings were obtained at the early stage of this investigation: mobile users can fundamentally access their applications differently, and the application name, location of usage and telephone number may provide more discriminatory information towards a classification process than other application features. A preliminary study was formed to examine the effectiveness of the applications features by employing three classifiers (the RBF, FF MLP and a rule-based approach) with a sub-dataset containing 20 random users' telephony activity. Based upon the experimental results, the dialled telephone number and location of calling features have been proved to contain contributory information towards the classification results. Also, the experimental results show that the rule-based approach is the most suitable classifier to solve this problem because of its performance and efficiency. Larger FRR figures suggest that a dynamic profile should be employed to solve the template ageing problem and a smoothing function should be put in place to cope with the inconsistency of a user's behaviour.

By employing the combination of the rule-based approach, both the static and dynamic profiling techniques and a smoothing function, the complete experiment on users' applications (intra-standard, intra-extended and multi-instance) was conducted. Among a total of 60 sets of configurations, with a classifier configuration of the dynamic profile with 14 days[5] most recent

[5] Multi-instance applications employed 10 days

user activities and the smoothing function of 6 entries, the rule-based approach obtained the best performance of an EER of 13.5%, 5.4%, 2.2% and 10% for the general application, telephony, text messaging and multi-instance applications usage respectively. Therefore, these techniques are viable as a behaviour profiling security mechanism within the mobile host environment. The verification process could be carried in the background while mobile users utilise their applications; if several abnormal activities occurred within a fixed time frame, further security processes would be initiated according to the level of the incident. Based upon the success of these experimental results, the next chapter will focus upon designing a behaviour profiling verification architecture that could accommodate the aforementioned behaviour profiling verification techniques.

5 A Novel Framework for Behaviour Profiling on Mobile Devices

5.1 Introduction

Having obtained a positive set of experimental results for users' applications behaviour within the mobile host environment in Chapter 4, it is important to design a novel security framework to facilitate the behaviour profiling technique and provide transparent and continuous protection for services and data hosted by the mobile device. This chapter describes a novel behaviour profiling framework, its processes and algorithms that will provide the transparent and continuous security protection required by the mobile device.

5.2 A Novel Behaviour Profiling Framework

In order to provide high level security to the mobile device with minimum user's inconvenience, a novel Behaviour Profiling framework which can provide transparent and continuous protection is proposed. The Behaviour Profiling framework primarily verifies a user's identity based upon which mobile applications they utilise. They will gain access to the device if they pass the verification process; otherwise, their access to the device will be rejected temporarily until they verify themselves through a secret knowledge based approach (i.e. random selected security questions). In order to provide adequate protection for the mobile device, the Behaviour Profiling framework must work in the following fashion:

- To improve the security for the mobile device beyond that offered by the knowledge based approach;
- To continuously verify the user's identity based upon which mobile applications they utilise;
- To ensure the verification process is carried out in a user-friendly manner: the user is mainly verified in a transparent way rather than being verified intrusively;
- To provide an architecture which can operate in one of three modes based upon the desired output implementation: as a standalone security countermeasure; within an IDS system as a misuse detector; or within a transparent authentication mechanism.
- Also, the architecture would be suitable for every mobile device regardless of hardware configuration, processing power or network capability.

These objectives have been achieved by utilising the combination of engines and processes within the novel Behaviour Profiling framework as illustrated in Figure 5.1. As mentioned earlier, the Behaviour Profiling framework verifies a user's identity based upon their application activities; and

the entire verification procedure is carried out by the cooperation of the process engines and the Security Manager. First of all, the Data Collection Engine gathers a user's application activities and transforms them into various behaviour input samples. Then, the Behaviour Classification Engine performs the verification process by comparing the input sample(s) with suitable profile(s) which is(are) generated by the Behaviour Profile Engine. Once the verification process is completed, the verification result will be processed appropriately by the Security Manager according to the mode in which the framework operates. When the framework operates in standalone mode, the Security Manager handles the verification result by itself and makes any necessary corresponding responses, such as associating appropriate labels for the verified input data (whether legitimate or illegitimate) and updating the SS level. When the framework operates in dependent mode, the Security Manager simply forwards the verification result to a more comprehensive security mechanism (e.g. TAS) and the corresponding security mechanism makes any final decisions accordingly. A detailed description of this process is thoroughly explained throughout the rest of this chapter.

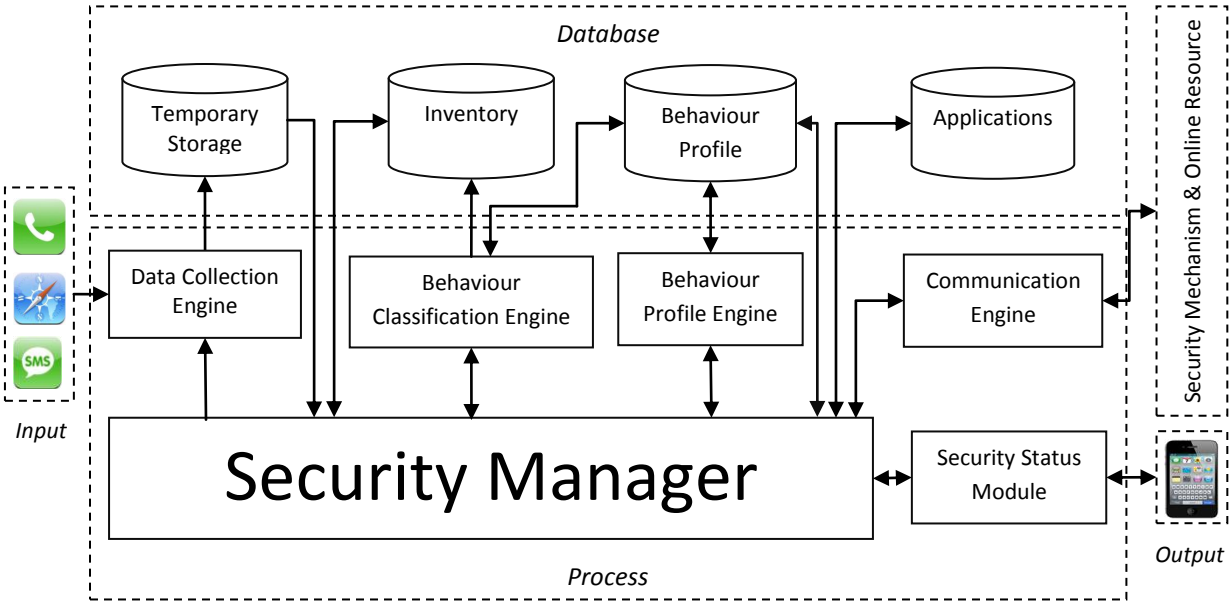


Figure 5.1: A novel Behaviour Profiling Framework

5.3 Processing Engines

The proposed Behaviour Profiling Framework relies on a number of processing engines: Data Collection Engine, Behaviour Profile Engine, Behaviour Classification Engine and Communication Engine to carry out various tasks, such as collecting data, generating profiles, verifying users' activities and contacting other security mechanisms. Each of these engines and their functionalities will be fully discussed in this section.

5.3.1 Data Collection Engine

The main duty of the Data Collection Engine is to capture mobile users' applications activities. When an application is utilised by a user, the Data Collection Engine (as illustrated in Figure 5.2) automatically gathers the information associated with that application in the background of a mobile device OS. This information can be either related to the system level information of that application or personalised user data. The system level information of the application can be the name of the application, date, time and location of usage; while the user related application information can be any information entered by the user, such as telephone numbers, URLs and email recipients. According to applications feature details stored in the Application records table[6] (as demonstrated in Table 5.1) within the Application database, the Feature Identifier extracts information and form it into various features. For instance, when a web browser is utilised, the information associated with the name of the application, date and time of accessing, location of usage and the URL which the user enters will be extracted into features according to the information provided by the Application records table.

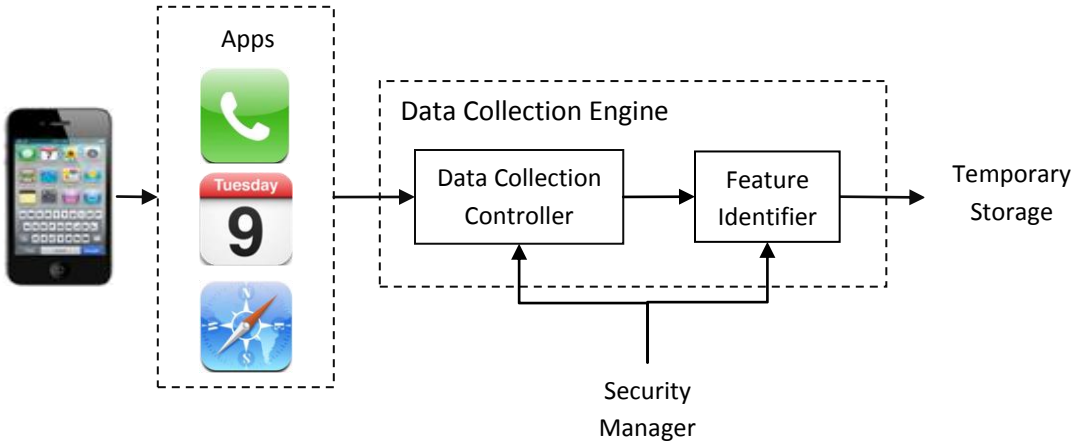


Figure 5.2: Data Collection Engine

ID	App_Name	Category _ID	Feature _1	Feature _2	Feature _n	Verification _status	Profile	EER	Collect
1	Clock	1	1	-	-	1	1	19%	1
2	Calculator	2	1	-	-	0	0	-	1
3	Telephone	3	1	2	-	1	1	5%	1
4	SMS	3	1	2	-	1	1	3%	1
5	Safari	3	1	3	-	1	0	-	1
:	:	:	:	:	:	:	:	:	:

Table 5.1: Applications record

[6] All the database tables in this thesis are created for illustration purposes.

The information about application features and categories is initially preloaded on the mobile device based upon their OS because different mobile platforms may host applications differently. As more than 15,000 new mobile applications are becoming available every month, the feature identification process that involves identifying which category an application belongs to and which features should be extracted from it can be a difficult task. It would be virtually impossible for each mobile user to manually carry out the identification process when a new application is installed on their device. Therefore, the feature identification process should be carried out by the Feature Identifier automatically without any user's assistance. In order to achieve this, two possible solutions have been taken into consideration. The first solution is to employ a central network based application features repository. The repository will contain all necessary information to facilitate the feature extraction process and it will be managed by an independent source. When an application is downloaded and then installed, the framework will download the feature set information of that application from the repository and update the Application record table accordingly. As a result, the Feature Identifier can extract the information correctly when a new application is utilised. The second solution is to create an intelligent feature identification component within the proposed framework. The proposed feature identification component would identify which category an application belongs to and which features should be extracted from that application. However, it would require a certain amount of application information before establishing which category an application belongs to and what features are associated with it. As a result, verification processes for that application cannot be accurately performed during the feature identification period. In comparison, details of an application can be quickly updated in the Application Record table straight after that application is installed on the device by utilising the first method; then the Feature Identifier can exactly extract information of that application when the user uses it. As a result, the first method will be employed as the preferable solution for assisting application the feature identification and extraction process.

Once the Feature Identifier extracts all necessary application features, the Data Collection Engine then proceeds to the next phase, pre-processing these application features into a biometric sample. The Data Collection Controller then sends the behaviour sample to the Temporary Storage for further processing. The actual size of the Temporary Storage varies depending upon the way in which the Behaviour Classification Engine performs the verification process (which is discussed in section 5.3.3). Once the verification process is performed, the data stored in the Temporary Storage will be removed accordingly. Nonetheless, Temporary Storage should have same structure for each mobile device regardless of hardware configurations; the Temporary Storage table

contains several data fields, such as the date, time, the name of the application and various features. Table 5.2 illustrates an example of the Temporary Storage with a number of application entries.

ID	Date	Time	Application_Name	Feature_1	Feature_2	…	Feature_N
1	01/09/11	07:31	Clock	325.689	-	…	-
2	01/09/11	08:55	Telephone	653.142	07875610456	…	-
3	01/09/11	13:23	Text_message	633.142	07773156895	…	-
4	01/09/11	14:55	Safari	639.145	www.bbc.co.uk	…	-
:	:	:	:	:	:	:	:

Table 5.2: Temporary Storage

When verification is required, the Temporary Storage forwards all input data to the Security Manager. According to the Application Features Record (as demonstrated in Table 5.3), the Security Manager replaces the raw information stored in the input data with appropriate IDs accordingly and then stores it in the Behaviour Input Data table (as shown in Table 5.4). In this way, a significant amount of data storage can be saved; also the process speed will be improved when the data is required by any subsequent usages. When any raw information could not find a match either within the Application_Name column in the Application Name (as demonstrated in Table 5.6) or within the App_Feature_information column in the Application Features Table (as demonstrated in Table 5.7), such as when a new application is installed and new features associated with it, a new record will be created in the table accordingly to accommodate that raw information; both tables are stored in the Applications database. Depending upon whether an application is verifiable or not (as described in Table 5.4), the input data will be either forwarded to the verification process which is carried out by the Behaviour Classification Engine if its verification status is labelled with 1 (verifiable); or the information will be directly transferred to the Behaviour Profile database in the Behaviour Audit table for the archiving purpose if their verifiable status is labelled with 0 (not verifiable). All applications' verifiable status is marked with 1 by default. However, the verifiable status of an application can be modified through the Security Manager if necessary. For instance, the nature of the camera application is to take pictures of new things which are difficult to predict. If a user has not been verified by their camera usage for a period of time, a suggestion can be made to the user to change the verifiable status of the camera application to not verifiable.

ID	App_Feature_ID	App_Feature_information
1	1	323.689
2	1	563.485
3	2	07852398652
4	3	www.plymouth.ac.uk
5	1	956.523
6	3	www.bbc.co.uk
:	:	:

Table 5.3: Application Features Record

ID	Date	Time	Application Name	Feature_1	Feature_2	…	Feature_N	Verifiable
1	01/09/11	07:31	1	1	-	…	-	1
2	01/09/11	08:55	2	21	3	…	-	1
3	01/09/11	13:23	3	10	7	…	-	1
4	01/09/11	14:55	4	17	11	…	-	1
5	02/09/11	08:23	5	1	-	…	-	0
:	:	:	:	:	:	:	:	:

Table 5.4: Behavioural Input Data

ID	App_category
1	Inter
2	Intra_standard
3	Intra_extended
:	:

Table 5.5: Application Category

ID	Application_Name
1	Clock
2	Telephone
3	Text_message
4	Safari
5	word
:	:

Table 5.6: Application name

ID	Application_Feature
1	Location
2	Telephone number
3	URL
:	:

Table 5.7: Application Features

5.3.2 Behaviour Profile Engine

The primary function of the Behaviour Profile Engine (as illustrated in Figure 5.3) is to generate various behaviour profile templates. This is achieved by utilising a combination of the user's historical behaviour data and a number of templates generation algorithms.

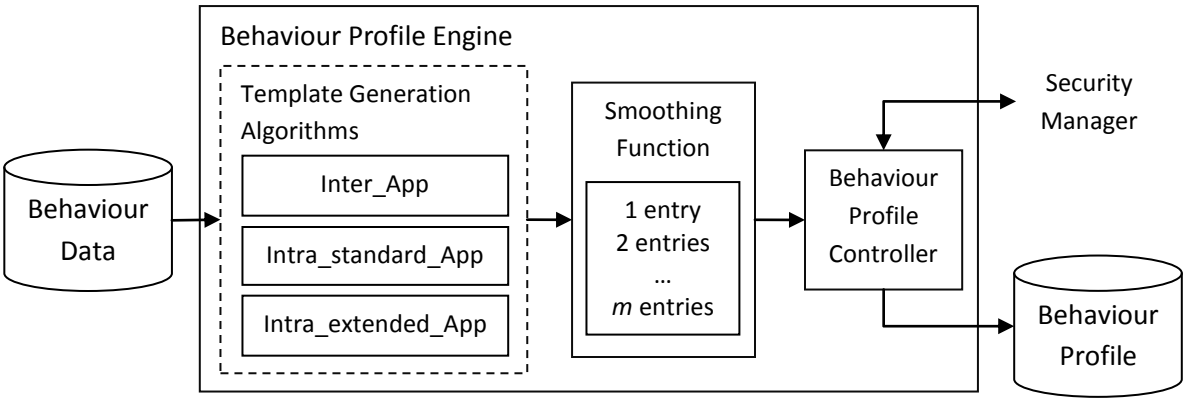


Figure 5.3: Behaviour Profile Engine

The initial profile template generation process can be a tricky task for any biometric based security system. Due to the nature of the behaviour profiling technique, the proposed framework has to gradually collect a user's behavioural data over a period of time rather than gather all information at the device registration stage. From the results and observations obtained by experiments of Chapter 4, it demonstrates that a reasonable level of system performance can be achieved by utilising profiling data containing 150 application activities. As a result, it suggests that the framework should collect a minimum of 150 application entries after the initial device registration phase. During the enrolment period, the framework will automatically gather a user's application activities by utilising its Data Collection Engine in the device background. Also, during the same period, the framework will not be able to provide any security protections for the device due to incomplete profile templates. Therefore the device security has to rely upon other security mechanisms, such as PINs.

Once a sufficient amount (i.e. more than 150 applications entries) of data is collected, the Behaviour Profile Engine will start to generate application profiles by utilising the three template generation algorithms for inter[7], intra-standard and intra-extended applications accordingly. For inter applications, a generic profile containing all the applications' location usage and dates of access will be created. In this way, when an application that has not got its own profile is utilised, such activity will not be simply rejected by the framework; thus, user convenience is improved. For intra-standard applications, each has their own profile containing locations of usage and dates on which they were accessed. For intra-extended applications, they also have their own profiles containing utilisation locations, dates of use and extra associated information. When the initial template generation phase is completed, all the generated application templates will be stored in

[7] An inter application is an intra-standard application without their own profile

the Behaviour Template table (as demonstrated in Table 5.8) within the Behaviour Profile database. By utilising these templates and imposter's data, the EER of each applicationcan be obtained accordingly. Also, these templates will be used by the Behaviour Classification Engine in any subsequent verification processes.

ID	Generation Date	Application_ID	ERR	Freshness	Template Storage	Others
1	11/09/11	1	5.3%	0.86	\\profile\ 1	-
2	13/09/11	2	2%	0.95	\\profile\ 2	-
3	15/09/11	3	7%	1	\\profile\ 3	-
4	11/09/11	4	1%	0.86	\\profile\ 4	-
5	12/09/11	5	17%	0.91	\\profile\ 5	-
:	:	:	:	:	:	:

Table 5.8: Behaviour Template

The imposter data is preloaded when the proposed framework is implemented on a device. Also, the data needs to be updated regularly to ensure its quality. This can be achieved by downloading the latest imposter data from a central imposter data repository which is described in full detail in section 5.3.4. Alternatively, the imposter data can be automatically generated using traditional statistical tools by the proposed framework itself (Jain *et al*, 1999). For instance, the Behaviour Profiling framework can replicate the legitimate user's data into artificial imposter data by utilising the bootstrapping method. In this way, a significant amount of imposter data downloading can be avoided. Nonetheless, the quality of the artificial imposter data is highly dependent upon the legitimate user's data and the generation method utilised.

All user application usage is stored in the Behaviour Audit Log table (as illustrated in Table 5.9) within the Behaviour Profile database. The details of the application usage includes: the date and time of utilisation, the application ID, the verification success (whether an activity passed the verification process (1), failed the verification process (0), or not available (-1); or an activity is collected during template generation process (2)) and a number of the application features. The Behaviour Audit Log table starts to populate its records as soon as the template generation process begins. During the template generation phase, the verification status of every application usage record is labelled with 2 as all user activities are assumed to be legitimate but they have never been verified. Once the initial template generation stage is completed, the framework will check the usage of each application based upon their verification status (as demonstrated in Table 5.4). If their verification status is not verifiable, their verification success status will be marked with -1 straight away. If their verification status is verifiable, the verification success status of that usage record will be labelled with either 1 or 0 depending upon its verification result. The data

stored in the Behaviour Audit table can be utilised to provide general feedback to the user, such as showing how many applications were used and their verification results during a period of time. More importantly, all application activities being verified successfully will be utilised for the template re-generation process. As a result, the behaviour data will have to be stored for a minimum of the profile duration period. However, the maximum period of how long the behaviour data should be kept depends upon each individual user's preference and the capability of their mobile device.

ID	Date	Time	Application_ID	Verification Success	Feature_1	Feature_2	Feature_n
1	11/09/11	09:23	1	2	6	-	-
2	11/09/11	09:25	1	2	23	1	-
:	:	:	:	:	:	:	:
103	11/10/11	10:15	4	0	15	-	-
104	11/10/11	11:22	2	-1	15	-	-
105	11/10/11	15:30	5	1	7	5	-
:	:		:	:	:	:	:

Table 5.9: Behaviour Audit Log

As mentioned in Chapter 3 (section 3.2.1), biometric systems rely on high quality generated templates to produce accurate verification outcomes. Also, behavioural biometric characteristics tend to change under various circumstances. In order to maintain templates of a mobile application at a high level of quality, a dynamic profiling technique is employed: application templates are generated by using the most recent *n* days of a user's historical behaviour data. Accordingly to a user's daily usage, all successful verified records will be included in the automatic application template regeneration process at the end of each day; while for those applications which did not get any successful verifications throughout the day, their templates will stay the same as the last time when they were updated/generated. In this way, users will always have an accurate profile containing their recent activities. Also, once templates of an application are regenerated, the Behaviour Template table will be updated accordingly with the latest template and EER status of the application.

It is envisaged that the freshness of each template may have a differing impact upon the verification process: more recently generated templates should carry a bigger weighting towards the verification result while older templates should be given a smaller weighting for the verification result. Therefore, a numerical value for the freshness of the template is employed to improve the performance of the framework; the freshness of the template is obtained by utilising the following formula:

Freshness = (n - number of days since the template was generated)/n

where n is the number of days employed in the template generation process

The templates' freshness is calculated on a daily basis straight after the template regeneration process. A template will be removed from the Behaviour Template table when its freshness equals zero (i.e. the template is out of date). When the Behaviour Template table is empty, the user has to perform the enrolment process to repopulate templates again. For instance, if 10 days is chosen for a user's profile duration, after two weeks' holiday (assume the mobile device is not in use during this period), that person will have to carry out the enrolment process once again to generate new profile templates as their existing templates are considered obsolete.

As demonstrated by the experimental results presented in Chapter 4, system verification performance can be improved significantly by utilising more log entries. Therefore, the framework utilises a smoothing function by employing *m* (where *m* is an integer > 0) consecutive application activities as one verification input. Moreover, experimental results of Chapter 4 suggest that the larger the *m* value is, the better the system performance would be; this means that a long verification time might be needed if the framework chose a large value for m. Such an incident would provide opportunities for potential misuse. By employing the template of each individual application and the imposter's data, an EER for verifying these *m* applications can be obtained for each of the smoothing techniques as shown in Table 5.10.

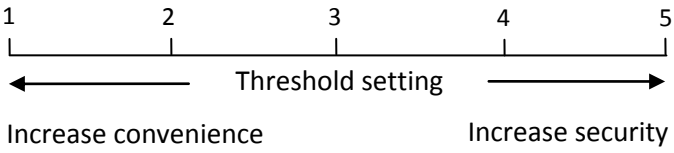
ID	Number of applications	EER
1	1	16.5%
2	2	13.5%
3	3	12.1%
:	:	:

Table 5.10: Smoothing Function

Table 5.10 shows various system performances when a different number of applications' activities are employed by the smoothing function. For instance, the system achieves an EER of 13.5% when the smoothing function utilises 2 applications' activities as input data for the verification process. More importantly, these system performances (i.e. EER) will be utilised as threshold reference points when the Behaviour Classification Engine performs verification processes. For example, when the Behaviour Classification Engine verifies three applications it will use 12.1% as a threshold (according to Table 5.10).

As described in Chapter 3, the threshold is a critical parameter for a biometric system as it determines the level of security the system provides versus the level of convenience a user gets:

higher levels of security would have legitimate users being rejected more often, while lower levels of security would allow imposters to gain access more easily. Therefore, the proposed framework employs a dynamic scaling threshold setting allowing users to flexibly choose their threshold setting based upon their security requirement.



As shown above, the threshold includes five setting scales: more convenient, convenient, normal, secure and more secure represented by 1, 2, 3, 4 and 5 on the scale respectively. Among these five scales, the normal scale represents a reference point for threshold settings. At the normal setting, the system threshold for each user is the EER of their smoothing function. When the threshold setting slides up or down by one point, the threshold will be increased or decreased by *x*% (where *x*>0, e.g. 5) of the EER value of the smoothing function accordingly. At the device registration phase, a user is required to select which security level they prefer to have for their devices in general, where the normal setting is chosen by default. Also, each option is accompanied with descriptions which allow the user to understand in non-technical terms what these options represent.

5.3.3 Behaviour Classification Engine

The Behaviour Classification Engine provides the main functionality for the verification process. When a verification requirement (as demonstrated in Figure 5.4) is met, the Behaviour Classification Engine calculates a temporary value for the input application activity (obtained from the Behavioural Input data table) by utilising their profile (stored in the Behaviour Template table). The temporary value will be compared with the predefined threshold: within the threshold, the activity will be assumed as legitimate; if exceeding the threshold, the activity will be classified as illegitimate. Then, the Behaviour Classification Controller sends the labelled activity data to the Behaviour Audit table and forwards the verification result to the Security Manager which will make a response based upon the operation modes of the framework, discussed in section 5.6.

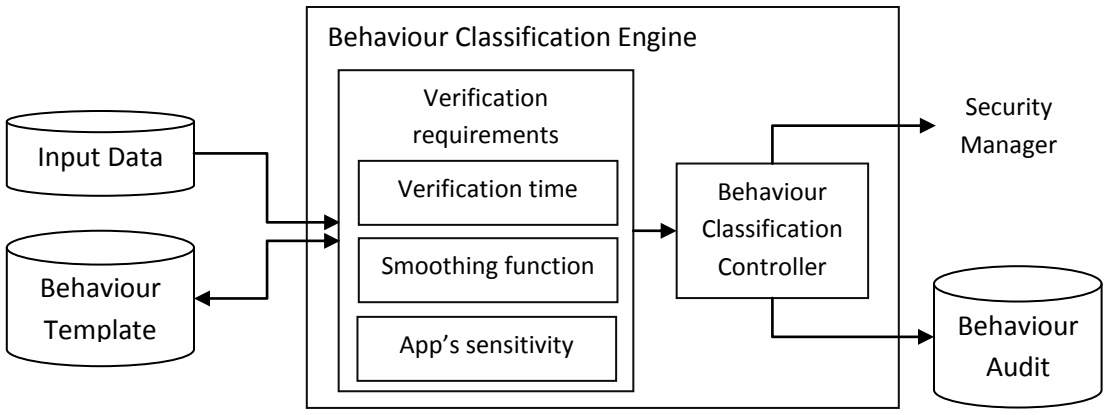


Figure 5.4: Behaviour Classification Engine

The Behaviour Classification Engine performs verifications based upon one of the following criteria and the checking processes are depicted in Figure 5.5:

- The requirement of the smoothing function: the Behaviour Classification Engine utilises the smoothing function to verify a number of applications' activities (e.g. six applications) as one input to achieve the best possible system performance.
- The verification time: to gather a desired number of applications' activities may be time consuming and this would open the potential for misuse. However, this problem can be minimised by employing the verification time requirement which forces the Behaviour Classification Engine to perform verifications even if the desired number of applications' activities are not collected.
- The sensitivity of the application: is used by the Behaviour Classification Engine to improve a user's convenience when they require access to high value applications but the current SS level is below 2.

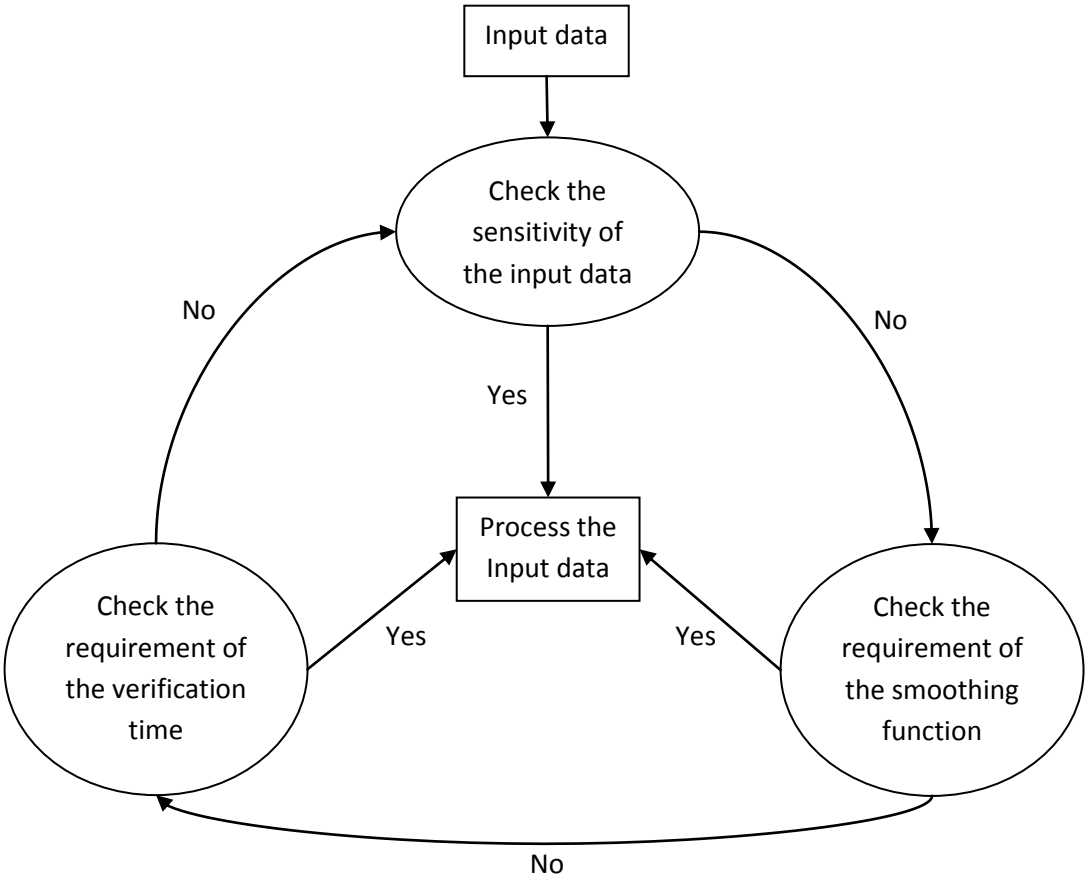


Figure 5.5: the verification requirement checking processes of the Behaviour Profiling Engine

The experimental results presented in Chapter 4, demonstrate that the behaviour profiling system can achieve its best performance by utilising 6 applications for the smoothing function. Hence, the requirement of the smoothing function is that verification can be processed when 6 application activities are gathered. When an application is utilised, the Behaviour Classification Engine will not perform verification but wait for the user to access another application; when the total number of applications reaches 6, the Behaviour Classification Engine will verify these 6 applications' activities.

The verification time is the time period that controls how long the Behaviour Classification Engine can take to perform verification on a number of applications; it is chosen by the user at the registration phase. As soon as an application is utilised, a verification timer will be automatically started. When the timer is smaller than the verification time, the Behaviour Classification Controller compares the total number of applications with the requirement of the smoothing function (i.e. requires 6 application activities); when the requirement of the smoothing function is

met, these application activities will be verified by the Behaviour Classification Engine; otherwise, the Behaviour Classification Engine will have to wait until the total number of application activities reaches to 6. When the timer equals the verification time, the Behaviour Classification Engine will verify the application activities even if the requirement of the smoothing function is not met. By employing the verification time as a reference, this forces the framework to make a security decision within the reference timeframe even though the total number of applications has not met the requirement of the Smoothing Function. Therefore, the framework will always provide security within a reasonable timeframe.

The third requirement that enables the Behaviour Classification Engine to perform verification is the sensitivity of the application. When a user requests access to a high value mobile application but the SS level is below 2, the Behaviour Classification Engine will verify any applications which have not been verified before and update the SS level even though the total number of applications has not met the requirement of the smoothing function or the timer is less than the verification time. If the updated SS level meets the security requirement for access to the high value application, the user will be granted access. Otherwise, the user will be challenged with a randomly selected security question. In this way, a level of user's inconvenience will be reduced.

5.3.4 Communication Engine

The Communication Engine acts as an interface between the framework and the application features repository, the imposter behaviour database and other security controls (as demonstrated in Figure 5.6). By utilising the Communication Engine, the framework can easily update the application information and the imposter data through a wireless link (e.g. a Wi-Fi connection), and communicate with other mobile security controls internally within the mobile device when the framework operates in dependent mode.

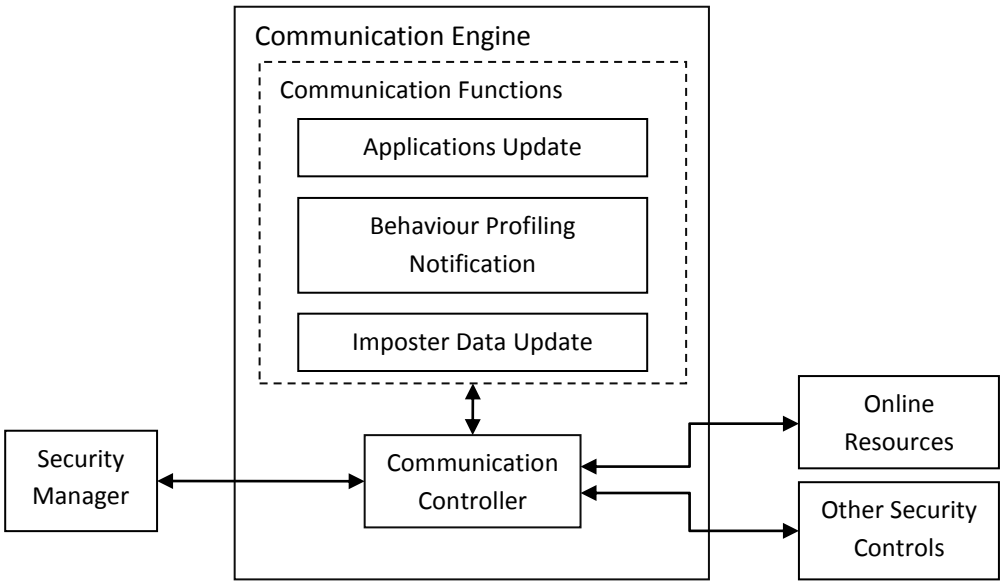


Figure 5.6: Communication Engine

The online application features repository (as described in section 5.3.1) contains the category of each application (either inter, intra-standard or intra-extended) and the details of their features. The online application features repository updates itself regularly as new mobile applications become available on a daily basis. When a new application is installed by a user, the framework checks if the details of that application are already stored in the Application records; if not, the framework will utilise the Communication Engine to communicate with the online application features repository and request information for that application. By utilising the application information updated in the Application record, the framework will be able to determine which information should be extracted into various features for this new application when it is used by the user.

The imposter behaviour database is a collection of anonymous users' mobile applications activities. These activities can be utilised as imposter data for obtaining the EER of the system for individual mobile users: obviously one user's normal applications usage will become abnormal activity on another user's mobile device. Be default, the framework is equipped with imposter data for calculating the EER of the system at the template generation/regeneration stages. According to Flurry (2009), a user's mobile application activities tend to change after a period of time; depending upon individual users, some may change in a shorter period (e.g. 10 days) while others may take a longer period (e.g. 30 days). As a result, some elements of the imposter data could become less relevant to the user's current application activities and may result in a lower system FAR; this will potentially affect system performance by increasingly rejecting legitimate user's

application usage. Therefore, when the system FAR rate exhibits a steady decrease over a period of time, it is a good indication that the framework should update its imposter data. At that moment, the Communication Engine will send a request to the imposter behaviour database to obtain the latest relevant imposter data samples and update the existing imposter behaviour dataset.

As demonstrated in Figure 5.6, apart from the Applications Update and Imposter Data Update functions, the Communication Engine has another function: Behaviour Profiling Notification. The Behaviour Profiling Notification function has two sub functions: sending lockdown codes and outputting verification results. Only one of them will be utilised according to the operation mode of the framework which is discussed in section 5.6. In standalone mode, the framework locks down the device after several security breaches. Then the Security Manager generates a lockdown code. Depending upon the nature of the ownership of the device, the Communication Controller will send the code to an appropriate destination. If the device is owned by a company, the code will be sent to the system administrator of the company; if the device is for personal use, the code will be sent to the user's appointed destination, obtained from the owner at the device registration phase. When the framework operates in dependent mode, the framework works as a component for a more comprehensive security management system (e.g. TAS). As a result, the Communication Engine functions in a simpler manner: it forwards verification results provided by the Security Manager to the corresponding system. How the security management system treats the result depends upon its own configuration which is not covered by the proposed framework; however, examples of corresponding systems are discussed in section 5.6.2.

5.4 Security Status Module

The Security Status Module has two major functions: providing general feedback information to the user and calculating the SS level. For general feedback information, it includes: when, where and which application(s) the user used over a period of time and the verification results from this usage (whether passed or failed). Despite not every user viewing the information offered by the Security Status Module, it does provide a useful insight which may show the user how their device is utilised and therefore help them to identify possible misuse.

The SS level constantly indicates what security setting the system is at. The SS level is used by the framework to monitor how secure a system is and provide or deny access to a user accordingly. When the SS level meets security requirements, access to the mobile device will be granted. The

SS level is a numeric value in the range of -3 to +3: -3 indicates low security whilst +3 indicates high security[8]. When the device is initially used, the SS level is set to 0, the normal security level. Subsequently the SS level will fluctuate based upon two critical factors: the application performance factor and the verification result. The application performance factor is dynamically allocated to each application based upon their performance in terms of EER. As demonstrated in Table 5.11, applications with better performance are given bigger factors, while applications with poorer performance are allocated smaller factors. Also, if the performance of an application changes, the performance factor of that application is altered accordingly. Moreover, due to different usage patterns, users might get different performance factors even for the same application.

Application Performance (EER)	Factor
0-2%	1
2-4%	0.9
4-6%	0.8
6-8%	0.7
8-10%	0.6
10-12%	0.5
12-14%	0.4
14-16%	0.3
16-18%	0.2
>18%	0.1

Table 5.11: Application Performance Factor

After the activity of an application is verified, a temporary value will be allocated to the performance factor of that application. When a verification process involves more than one application, the temporary value will be obtained by adding the performance factor of each individual application together. For instance, if three applications A, B and C are utilised by the Smoothing function and their performance factors are 0.5, 0.7 and 0.6 respectively, the temporary value equals the summation of these three applications' performance factors (i.e. 1.8). Depending upon the verification result, the temporary value is then added to (verified successfully) or subtracted from (verified unsuccessfully) the existing SS level to derive the current SS level as shown in Figure 5.7.

$$Current\ SS\ level = \sum_{i=1}^{m} VR \times\ APF_i + Existing\ SS\ level$$

Where VR=Verification result, APF= Application Performance Factor, m= number of applications

[8] The boundaries defined on the numerical scale are only provided as a suggestion. In practice, these values may be redefined.

Figure 5.7: The SS level calculation process

The time that has elapsed between two verification processes also affects the SS level. It is important that when a device is not used for a period of time, its SS level should be reduced accordingly. In this way, the opportunity of a device being abused would reduce significantly when the device was left with a high SS level for a while. The formula for degrading the current SS level when the device is not used for a period of time is illustrated in Figure 5.8. The Time Period is an average duration between two applications being utilised by a normal mobile device user. Based upon users' activities presented in Chapter 4, analysis was carried out and found that a typical Time Period is around 50 minutes, meaning an application is utilised by a mobile user every 50 minutes on average (care should be taken on this suggestion as the figures were obtained in 2004; it is highly likely that people now interact more often with their mobile devices compared with a few years ago). Hence, it is suggested that the actual Time Period employed by the framework should be smaller than 50 minutes. The time factor does not have any influence on a negative Current SS level. The negative Current SS level can only be changed when a user's behaviour is verified or an Unlock code is entered.

$$Degradation\ function = Current\ SS\ level - \frac{Time\ elapsed}{Time\ Period}$$

Where Current SS level > 0;
When (Current SS level * Time period) <Time elapsed, SS level equals 0;

Figure 5.8: The SS level degradation function

By utilising this formula, two types of mobile users will receive more benefits from two different aspects: frequent users (convenient aspect) and infrequent users (security aspect). For the frequent users, their SS level should be kept at a high level most of the time as their SS level is updated regularly preventing the level dropping to 0; hence this provides more convenience if they want to access high value mobile resources which require with a high level system security (this is discussed fully in section 5.6.1). For infrequent users, their SS level should degrade to 0 well before they utilise another application. In this way, their systems are not left with a high SS level for a long time, preventing abuse of valuable mobile resources. The Time Period does play a significant role in the formula and it is not easy to define a universal time period for all mobile users; the actual Time Period depends upon what level of security an individual user requires and how often they utilise their devices. Nonetheless, the degradation function potentially opens an opportunity for misuse despite the one that is minimised by this process. Improving security in this

fashion will always have a trade-off and the improvement in user convenience does introduce this issue. However, this process of degradation helps to minimise it.

5.5 Inventory database

The Inventory database contains a number of tables which can be utilised by the system administrator for various purposes, such as checking the intrusive verification interface occurrence and updating the user's information. These data storage areas are the SS levels and user's information tables.

All changes of the SS level are stored in the System Security levels table as demonstrated in Table 5.12. Normally, the date, time, current SS level, updated SS level after an application is utilised and the application being utilised are stored in the System Security levels table. When the current SS level does not meet the security requirement (i.e. smaller than 2 when the user requests access to high value applications or smaller than -2 when the user tries to access normal applications), a randomly selected security question will be employed to verify the user's identity. For these scenarios, in addition to the normal details, the security question being utilised and the challenge outcome will also be stored in the table. When the user fails to answer the security question three times in a row, the device will be locked. As a result, an unlock code is required from the user before they can access any applications on the mobile device. The full details of this occurrence will be accordingly recorded in the System Security levels table.

ID	Date	Time	Current SS_Level	Updated SS_Level	App	Security_Question	Result
1	22/09/2011	22:45:31	0.1	-0.12	Clock	-	-
2	22/09/2011	23:10:50	1.5	2.2	Telephone	SQ_1	Pass
3	23/09/2011	10:36:10	-0.1	-0.05	Internet	-	-
4	24/09/2011	11:15:22	-2.1	-2.1	Files	SQ_5	Fail
5	27/09/2011	15:52:16	-2.1	0.51	Telephone	Unlock code	Pass
6	27/09/2011	18:53:12	0	0.3	Games	-	-
:	:	:	:	:	:	:	:

Table 5.12: System Security levels

By using the information stored in the System Security levels table, a graphical overview of the security status of the device during a period of time can be obtained. Also, possible intrusion can be identified by utilising the graphical feedback. Moreover, when the security question is frequently asked within a particular duration (e.g. 50 minutes) and the answer is provided correctly, a number of suggestions regarding potential problems can be provided by the framework to the system administrator:

- Problem with the template: the template for certain applications may not contain unique characteristics; therefore the template of the application should be regenerated.
- Problem with the threshold: the threshold may not be set properly; a re-adjusted threshold may prevent the question being asked frequently.
- Problem with an application: an application may not be classifiable after all; that application should not be considered for performing the classification process.

A user's information that is collected at the device registration phase is stored in the user's information table (as shown in Table 5.13). The information includes the user's name, a means of contact (e.g. email address) and a number of security questions. The user's name is utilised by the framework to generate greetings for each individual mobile device user. Also, from the administrator's perspective (when the device is deployed by a private organisation), they can generate a log of which users utilise what devices; the actual number of users will depend upon each individual private organisations and each user may have more than one mobile device. At the device registration stage, users are asked to complete a number of security questions (the actual number can vary depending upon the individual's preference). These security questions are employed to intrusively verify a user when the current SS level does not meet the security requirement. Also at the registration stage, a means of contact is required for the user which will be utilised to communicate a code to the user when the device is locked down. A user's contact could be either a mobile telephone number or an email address; texting can be used for sending the lockdown code if a device does not support the email service. Depending upon the ownership of the device, the lockdown code will either be sent to the user's pre-appointed contact address if the device is privately owned by the user; or the lockdown code will be sent to an administrator if the device is deployed by a company. By using the lockdown code, the user can unlock their device and start utilising the device again.

User Name	Andy
Email Address (telephone number)	Andy@li.com (07777123456)
1: What is your favourite colour?	Blue
2: Name your favourite restaurant	KFC
3: Memorable date	23011999
:	:

Table 5.13: User's information

5.6 Security Manager

The Security Manager is the brain of the framework as it controls all other elements. Based upon the working mode of the framework, the Security Manager has a variety of operational modes. These modes are discussed fully in the following section.

5.6.1 Standalone mode

In standalone mode, the role of the Security Manager includes:

- Continuously verifying the user's identity through their application activities
- Performing profile generation and re-generation on a daily basis
- Updating an application performance and the requirement of the smoothing function
- Calculating and maintaining the SS level
- Requesting an intrusive verification when the SS level falls below the security requirements and dealing with subsequent actions based upon the verification result.

The key task of the Security Manager is to monitor the current SS level and make subsequent decisions accordingly when a user requests access to an application. This is achieved by utilising the Process Algorithm as illustrated in Figure 5.9. The Process Algorithm is the core security component of the proposed framework. The Process Algorithm contains three main checking stages (as illustrated in Table 5.14) before the device is locked down (requiring a lockdown code from a system administrator or a PUK code from a cellular network provider to enable further use of the device). These checking stages were chosen to provide a high level of user convenience and improved security. The Process Algorithm employs a mixture of transparent and intrusive methods to verify a user's identity. The majority of legitimate users will experience transparent phases; while intrusive verification challenges are utilised to ensure users' legitimacy in the event of access being required to the mobile device but the SS level is below the set security requirements.

Checking Stage	Description
1	Check whether an application is protected
2	Check the current SS level
3	Intrusive verification if the current SS level does not meet requirements

Table 5.14: Three main checking stages

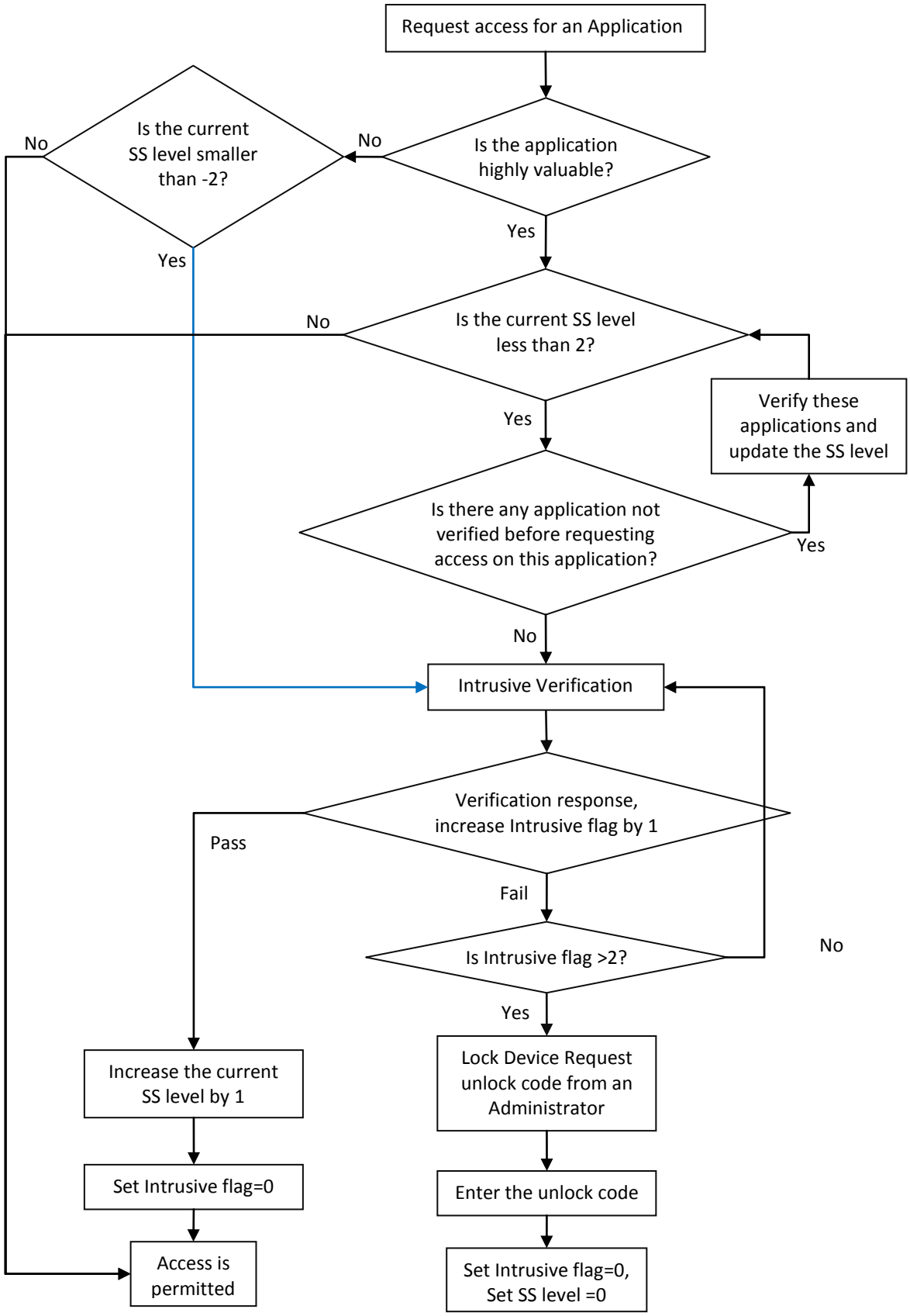


Figure 5.9: Security Manager: Process Algorithm

The Security Manager carries out a number of checks when a user requests access to an application. First of all, the Security Manager examines whether the application is a high value mobile resource. According to Ledermuller and Clarke (2011), a high value mobile resource is an application associated with high risk levels, such as corporate emails and e-banking applications. In order to protect high value applications, a security requirement is set: high value applications cannot be accessed when the SS level is below 2 unless the user passes an intrusive verification. In comparison, the security requirement for normal applications is more relaxed: users can gain access to them when the SS level is greater or equal to -2 unless the user is successfully verified through a randomly selected security question.

For the second checking stage, the Security Manger compares the current SS level with the security requirements for high value and normal applications. If the current SS level meets the requirements, the users will be granted access to that application. Otherwise, further checking will be performed based upon the nature of the application (whether it is a high value application or a normal application). If the application is a normal application, the user will be challenged with a randomly selected security question. If the application is associated with high value information, the Security Manger will make further examination of the situation: to check whether there is(are) any application(s) that has(have) not been verified before this high value application. If there are any unprotected applications, they will be verified first and the SS level will be updated accordingly. Then the user will be given access to the high value application if the update SS level is greater or equal to 2; and the user will be intrusively checked by a randomly selected security question if the update SS level is still less than 2. If there are not any unprotected applications being used before the high value application, the user will be intrusively verified by the randomly chosen security question.

For the final checking stage, the Security Manger utilises a randomly selected security question as the intrusive verification method to verify the user's identity. An intrusive flag that indicates how many times the intrusive verification method is utilised increases by 1 when the user answers the question; by default, the value of the intrusive flag is 0. The user will be granted access to the application if the question is correctly answered. Also, the current SS level will be increased by 1 and the intrusive flag will be set to 0. When the user fails to answer the security question correctly, the intrusive flag remains the same. Then the user will be challenged again if the value of the intrusive flag is not greater than 2. When the intrusive flag equals 3, the device will be locked down and only an administrative security password can unlock it. When a correct unlock code is

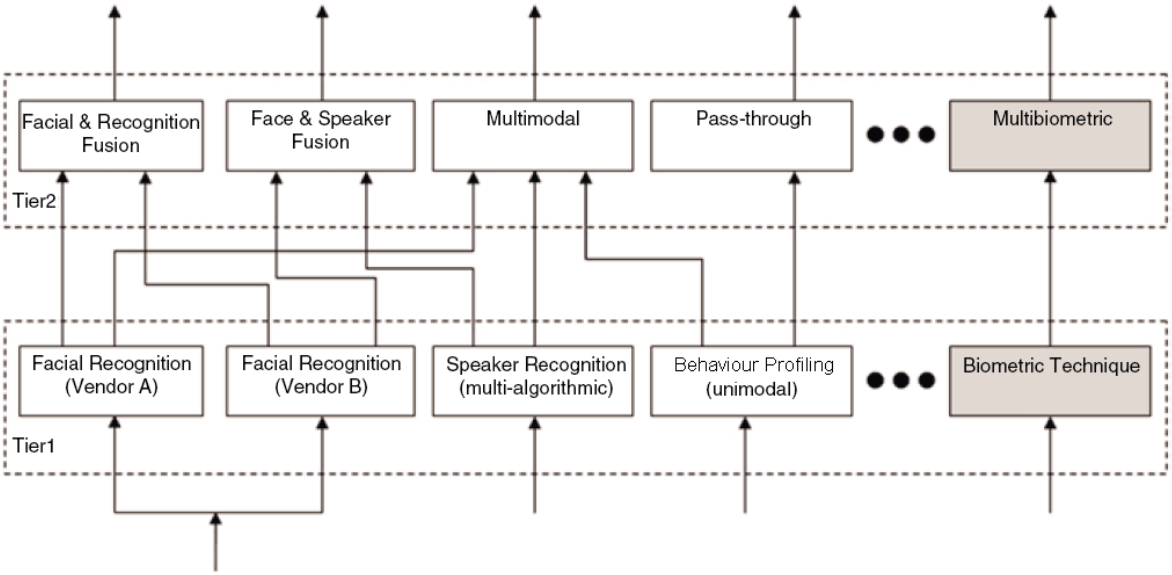
entered, the Security Manager will set both the intrusive flag and the SS level to 0 and the user will be able to access the device once again.

It is envisaged that if the system is working correctly, the SS level should be high enough to permit automatic access for legitimate users and their experience of intrusive security challenges will be minimised.

5.6.2 Dependent mode

The Behaviour Profiling framework is designed for two security purposes, either authentication or IDS. As a result, when it works in the dependent mode, it can become a component for an authentication security mechanism (e.g. the TAS) or an IDS security mechanism (e.g. the Knowledge-based Temporal Abstraction (KBTA) method (Shabtai *et al*, 2010)). In the dependent working mode, the Behaviour Profiling framework only provides a verification result and the final decision will be made by the other security mechanism.

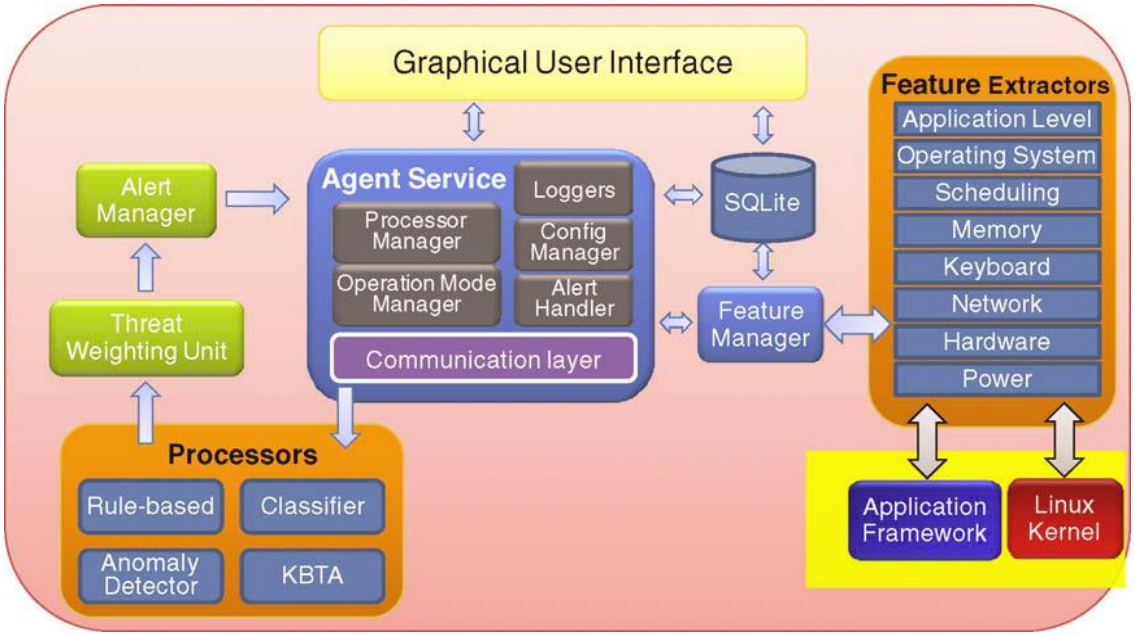
As mentioned in Chapter 3, TAS is an authentication system utilising a number of biometrics to provide transparent and continuous authentication for mobile users. This has been achieved by employing a two-tier approach: Tier 1 selects various biometric techniques and Tier 2 combines a number of multibiometric methods together (as shown in Figure 5.9). The Behaviour Profiling framework can be used as one of the biometric techniques in Tier 1 by TAS as it employs the way users utilise mobile applications to verify them; also, the Behaviour Profiling framework can provide unique contributions in operations of the Tier 2 to the TAS system. As the Behaviour Profiling framework verifies mobile users based upon their application usage, TAS can utilise its verification output alone in pass-through mode to provide transparent and continuous authentication. The Behaviour Profiling framework can also be used in multimodal mode when the Behaviour Profiling framework utilises the smoothing function with more than one application usage. In this case, the performance of the TAS system will be improved despite the authentication process requiring a longer time to complete. Moreover, the Behaviour Profiling framework can work with other biometric techniques to form a fusion mode in the TAS system. For instance, when a user sends a text message, their keystroke activities (i.e. how each character is typed into the message) and their behaviour profiling activities (i.e. where and who the message is sent) can be used in one fusion function. In this way, TAS can provide the authentication decision more confidently.



Source: Clarke, 2011

Figure 5.10: TAS two tier authentication approach

As described in Chapter 2, there are a number of IDS systems proposed to detect malware presence within the mobile device environment, such as the KBTA method. The Knowledge-based Temporal Abstraction method is a host based IDS. In addition, Shabtai *et al* (2010) proposed a host based IDS architecture to accommodate the aforementioned method (as depicted in Figure 5.10). Their evaluation indicates that the architecture works well for detecting mobile malware. Nonetheless, the architecture cannot detect any user related misuse. Therefore, the Behaviour Profiling framework and the architecture could work together to form a new host based IDS for mobile devices which can provide comprehensive detection of user misuse and also mobile malware. As a result, an alert will be raised not only when a device is infected by malware but also when it is misused by a user. Also, more accurate alerts would be generated when an application is infected by malware. For instance, when the text messaging service is infected by malware, it may send messages to a premium number without the owner's knowledge. If any messages were sent to the premium number, the Behaviour Profiling framework should detect the abnormal activity as it deviated from the user's normal behaviour. In addition, as the messages were generated by malware, the malware detection part of the IDS can also pick up the abnormal activity. Therefore, two alerts would be raised by the IDS system after an unauthorised text message was sent. This will improve the performance of the IDS system significantly.



Source: Shabtai *et al*, 2010

Figure 5.11: The Android HIDS architecture

5.7 Conclusion

In this chapter, a novel Behaviour Profiling framework which provides robust, transparent and continuous protection for mobile devices by verifying mobile users' application usage activities has been designed and the components and functionalities of the framework described in detail. By employing the dynamic profiling technique, the framework can generate a fresh user's profile allowing more accurate verification results to be obtained. By utilising the smoothing function, the framework reduces the impact of the high false rejection problem which every single behavioural biometric technique experiences; hence, the performance of the framework can be improved despite decision making taking longer to process. By assigning various security risk scores to different applications, the impact for each application towards the overall system security is controlled by the framework. As a scaled threshold setting was employed by the framework, a system administrator will be able to configure individual deployment based upon their security requirements. In order to improve a user's convenience as well as protecting the security of the device, the framework provides an additional level of verification by monitoring the SS level of the device. When the SS level is high, all mobile applications can be accessed; however when the SS level is low, only unprotected applications can be utilised. Also, a user's identity is not verified based upon a single pass or fail but a number of consecutive verification results. The framework can operate in different modes to serve a variety of purposes. When the framework operates in standalone mode, it verifies a user's identity and responds accordingly in isolation. When the

framework works in dependent mode, it provides verification results based upon user's activities, with the final decision being made by another security mechanism (either an authentication system or an IDS system). In the next chapter, the Behaviour Profiling framework will be evaluated in various scenarios via a simulation.

6 Evaluation of the Behaviour Profiling Framework

6.1 Introduction

This purpose of this chapter is to describe the evaluation process for the Behaviour Profiling framework proposed in Chapter 5. The performance was evaluated through a simulation approach utilising the MatLab environment rather than by developing a prototype on a mobile device. This enabled a complete validation of the processes and mechanisms over a far wider range of variables than would have been possible with an implemented prototype. The simulation process involved implementing the core functions of the Behaviour Profiling framework in standalone mode and verifying mobile users' applications activities utilising the same dataset identified in Chapter 4. This was a partial limitation on obtaining a realistic dataset. However, it offered the opportunity to directly compare the performance of the framework over the base experimental results. In order to examine the Behaviour Profiling framework, the following objectives were created:

- Examine the performance and effectiveness of the Behaviour Profiling framework towards verifying the user's identity and making subsequent decisions according to the verification output in a number of scenarios. The performance and effectiveness of the framework is then compared with the counterpart offered by the most widely used PIN authentication technique.
- Explore the relationship upon the level of security and usability when various variables within the framework are modified. Factors such as the smoothing function and verification time will be modelled to understand what effect they have upon system operation.

6.2 Simulation Implementation

For the simulation system, the majority components of the framework were implemented in the Matlab environment as illustrated in Figure 6.1. By utilising these components, the core functions of the framework, such as verifying a user's application activities, updating the SS level and making security decisions, can be thoroughly examined. Figure 6.1 also includes the Communication Engine which was not created due to time constraints. Nonetheless, this did not affect the simulation result at all, because the engine was not required due to:

- The simulation system was created for examining the framework functions within a standalone mode rather than in the dependent mode which requires the framework to communicate with other security mechanisms;
- All the application feature identification information was available as it was obtained in the experiments conducted in Chapter 4;
- The imposter data also existed within the MIT dataset since one user's applications activities can be utilised as the imposter data for another user.

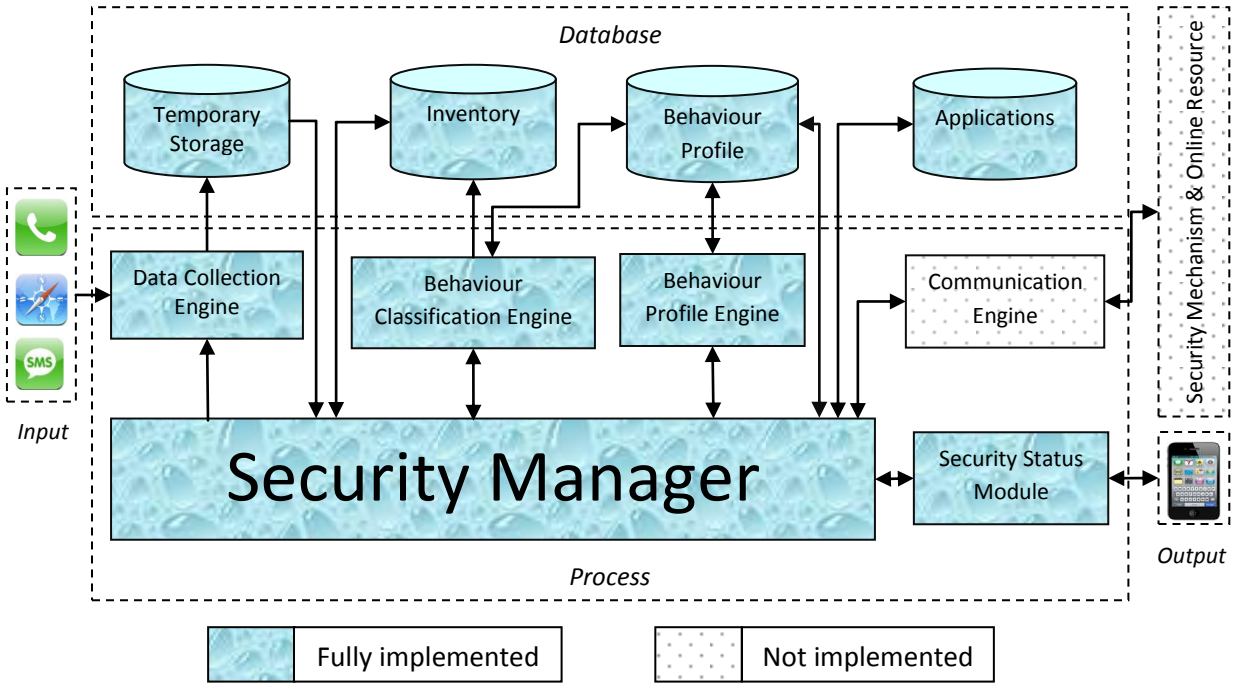


Figure 6.1: Simulation Implementation

In general, the simulation system contains five main components and two databases and they are the Data Collection Engine, Behaviour Profile Engine, Behaviour Classification Engine, Security Status module, Security Manager, Behaviour Profile database and Inventory database. The Data Collection Engine gathers users' applications activities, extracts various features accordingly to each application and converts these features into input data. The Behaviour Profile Engine employs the dynamic profiling technique as described both in Chapter 4 and Chapter 5: generating the user's profile by utilising their most recent 14-day applications activities and also the profile is updated on a daily basis. The 14-day profile duration was chosen as the experimental studies of Chapter 4 suggested that the best system performance can be obtained by utilising 14-day profiling data. The Behaviour Classification Engine employs the rule-based approach which was proposed and tested in Chapter 4 due to its outstanding performance and low computational

requirements. When any of the three verification requirements (the smoothing function, the verification time and the status of the application (whether an application is a normal or protected application)) proposed in Chapter 5 is met, the Behaviour Classification Engine compares input data with the profile of an appropriate application by utilising the rule-based approach. On the basis of the verification results and the performance factor of an individual application, the Security Status Module updates the current SS level accordingly; also, the user's input application activity will be either labelled with "legitimate user" or "imposter" according to the verification result and will be stored in the Behaviour Profile database for generating and/or updating a user's profile and updating the performance of an individual application. The Security Manager constantly examines the classification criteria and orders the Behaviour Classification Engine to perform the classification process accordingly. The Security Manager also continuously monitors the current SS level and assesses whether to grant the user's permission to access the mobile device or not. The Behaviour Profile database is employed for storing a user's application activities and profiles; while the Inventory database is mainly utilised for storing changes occurred for the SS level.

6.3 Simulation process

The entire simulation process was conducted within the Matlab environment. The simulation system employed the same 76 users' 4 weeks mobile activities which were utilised in Chapter 4's experiments as the simulation data. For each user, their activities were divided into two halves: the first half contains first two-week activities while the other half includes the last two-week activities. A user's profile was initially generated by utilising their first two-week activities and the profile was then updated on a daily basis. The second two weeks of users' activities were employed to evaluate the performance of the Behaviour Profiling framework for both legitimate users and imposters. As mentioned in Chapter 5, the Behaviour Profiling framework has several key parameters: the smoothing function, the verification time and the degradation function. The performance factor of each application also contributes to the SS level calculation process and plays an import role in the Behaviour Profiling framework as it directly affects the fluctuation of the SS level. Furthermore, the performance factor of the same application may vary for each individual user. Therefore, for the simulation process, each mobile user's applications performance was dynamically allocated based upon their experimental results presented in Chapter 4. The proposed Behaviour Profiling framework can also provide an extra layer of security for highly valuable applications by adding an additional security requirement (the current SS level should be greater than 2) when users require access to these applications. In order to evaluate the

effect of the Behaviour Profiling framework upon protected applications, the text message application was chosen to simulate one of the protected applications. As mentioned in Chapter 4, 22 users utilised the text message application during the chosen 4 week period and for the purpose of evaluation they have been selected as representing those mobile users who would like to add an extra layer of protection to their valuable mobile applications. Also, these 22 users' text usage represents 4.3% of the 76 users' total application usage.

Based upon the above simulation requirements, four scenarios were set up to evaluate the performance of the Behaviour Profiling framework. The performance is presented in terms of the probability of a legitimate user being asked a security question (and hence being falsely rejected (FRR)) and the probability of an imposter NOT being asked a security question (and therefore being falsely accepted (FAR)). For each scenario, their settings for the smoothing function and the verification time are illustrated in Table 6.1. In order to examine the roles in which the smoothing function and the verification time play, only one of them was changed between the two scenarios. Time periods for the degradation function were set between 1-60 minutes with a 10-minute interval for all four scenarios. The full sets of simulation results are presented in the next section.

Scenario A	Smoothing function: 1 application; Verification time: NA
Scenario B	Smoothing function: 3 applications; Verification time: 3 minutes
Scenario C	Smoothing function: 3 applications; Verification time: 6 minutes
Scenario D	Smoothing function: 6 applications; Verification time: 6 minutes

Table 6.1: Four scenarios for the simulation process

6.3.1 Simulation results – Scenario A

In Table 6.1, the framework was configured in the following manner for simulation scenario A: smoothing function: 1 application and verification time: not applicable. Based upon the verification requirement of the Behaviour Classification Engine (in Chapter 5), a user's application activity will be verified as soon as one application is utilised; therefore, the verification time is not applicable. For the same reason, none of the application activities were classified based upon the clause introduced by the Process Algorithm of the Security Manager (in Chapter 5 section 5.6.1): check if there are any applications not being processed before the protected application.

The simulation results for legitimate users and imposters in scenario A are presented in Table 6.2 and Table 6.3 respectively. By utilising 60 minutes as the time period for the degradation function, the best system performances for legitimate users are FRR of 8.6%, 74.8% and 11.45% for normal applications, the protected application and overall applications correspondingly; the high FRR for the protected application is due to the high security requirement for them which is the current SS

level needs to be larger than or equals 2. With the same set up, the system performance for imposters are FAR of 4.36%, 0% and 4.17% for their counterparts.

	The probability (%) of a legitimate user being asked by a security question (FRR)		
Degradation function	**Normal applications**	**Protected application**	**Overall (including normal and protected applications)**
1 min	9.05	98.89	12.91
10 mins	8.97	91.76	12.53
20 mins	8.88	85.9	12.19
30 mins	8.82	83.04	12.01
40 mins	8.71	79.87	11.77
50 mins	8.66	76.86	11.59
60 mins	8.6	74.8	11.45

Table 6.2: Simulation results of scenario A for legitimate users

	The probability (%) of an imposter NOT being asked by a security question (FAR)		
Degradation function	**Normal applications**	**Protected application**	**Overall (including normal and protected applications)**
1 min	4.35	0	4.17
10 mins	4.35	0	4.17
20 mins	4.36	0	4.17
30 mins	4.36	0	4.17
40 mins	4.36	0	4.17
50 mins	4.36	0	4.17
60 mins	4.36	0	4.17

Table 6.3: Simulation results of scenario A for imposters

6.3.2 Simulation results – Scenario B

As demonstrated in Table 6.1, the Behaviour Profiling framework was set up in the following fashion for scenario B: smoothing function set to 3 applications and verification time equal to 3 minutes. In comparison with the configuration of scenario A, scenario B employed more applications for the smoothing function; this provides the opportunity of allowing the smoothing function to work with up to 3 application activities. According to the requirements of performing verification by the Behaviour Classification Engine, within the 3 minutes verification time window, applications will be classified when the total number being utilised reaches 3. As soon as the verification time exceeds 3 minutes, even the total number of utilised applications is smaller than 3, these utilised applications will be verified by the Behaviour Classification Engine. As the smoothing function utilises a maximum of 3 applications, this provides an opportunity to improve user convenience if there are any applications not being processed before a protected application is utilised when the current SS level is smaller than 2.

Table 6.4 and Table 6.5 demonstrate the results for legitimate users and imposters from the simulation of scenario B. To maintain consistency between scenarios the degradation function utilises the same time period. Scenario B obtained the best system performance for legitimate users' normal, protected and overall application usage and they are FRR of 7.57%, 77% and 11.24% accordingly. By utilising the same configuration, the system performances for imposters' counterparts are FAR of 3.42%, 15.29% and 4.09% respectively. The FAR of 15.29% for the protected application is significantly higher compared with the result obtained by utilising the configuration of scenario A. This was due to using the smoothing function (to verify a number of application activities as one input) and the imposter gains the equal opportunity to reach a higher SS level as the legitimate users do despite the performance was improved on normal applications classifications.

	The probability (%) of a legitimate user being asked by a security question (FRR)		
Degradation function	**Normal applications**	**Protected application**	**Overall (including normal and protected applications)**
1 min	8.05	100	13.06
10 mins	7.87	94.28	12.53
20 mins	7.75	88.8	12.08
30 mins	7.72	85.95	11.88
40 mins	7.64	81.89	11.58
50 mins	7.62	78.57	11.38
60 mins	7.57	77	11.24

Table 6.4: Simulation results of scenario B for legitimate users

	The probability (%) of an imposter NOT being asked by a security question (FAR)		
Degradation function	**Normal applications**	**Protected application**	**Overall (including normal and protected applications)**
1 min	3.41	15.29	4.07
10 mins	3.42	15.29	4.08
20 mins	3.42	15.29	4.08
30 mins	3.42	15.29	4.08
40 mins	3.42	15.29	4.08
50 mins	3.42	15.29	4.09
60 mins	3.42	15.29	4.09

Table 6.5: Simulation results of scenario B for imposters

6.3.3 Simulation results – Scenario C

For scenario C, as illustrated in Table 6.1, the Behaviour Profiling framework was configured in the following way: smoothing function set to 3 applications and verification time equal to 6 minutes. In comparison with the setup of scenario B, scenario C utilised a longer verification time; this

increases the potential for allowing more application activities to be processed within one smoothing function. Based upon the requirement of the Behaviour Classification Engine, application activities will be classified as soon as the total number of them reaches 3 within the 6 minutes verification time window; when the 6 minutes verification time window is surpassed, even if the total number of application activities is smaller than 3, they will be processed by the Behaviour Classification Engine. Similarly to the setup of the scenario B for the protected application, scenario C also offers an opportunity to improve user convenience when they access a protected application when the current SS level is smaller than 2.

Simulation results of scenario C for legitimate users and imposters are presented in Table 6.6 and Table 6.7 accordingly. Again, by employing a time window of 60 minutes for the degradation function, the best system performance for legitimate users' normal, protected and overall application usages were achieved and they are FRR of 7.45%, 79.26% and 11.43% respectively. With the same framework setup, the system performances for imposters' equivalents are FAR of 2.47%, 26.39 and 3.97%.

	The probability (%) of a legitimate user being asked by a security question (FRR)		
Degradation function	**Normal applications**	**Protected application**	**Overall (including normal and protected applications)**
1 min	7.96	100	13.3
10 mins	7.83	96.23	12.89
20 mins	7.66	90.64	12.36
30 mins	7.63	87.8	12.15
40 mins	7.54	84.07	11.79
50 mins	7.51	80.85	11.58
60 mins	7.45	79.26	11.43

Table 6.6: Simulation results of scenario C for legitimate users

	The probability (%) of an imposter NOT being asked by a security question (FAR)		
Degradation function	**Normal applications**	**Protected application**	**Overall (including normal and protected applications)**
1 min	2.45	26.39	3.95
10 mins	2.46	26.39	3.96
20 mins	2.46	26.39	3.96
30 mins	2.46	26.39	3.96
40 mins	2.47	26.39	3.96
50 mins	2.47	26.39	3.97
60 mins	2.47	26.39	3.97

Table 6.7: Simulation results of scenario C for imposters

6.3.4 Simulation results – Scenario D

According to Table 6.1, the Behaviour Profiling framework was configured in the following manner for scenario D: smoothing function set to 6 applications and verification time equal to 6 minutes. Compared with the setup for scenario C, scenario D employed a higher number of applications for the smoothing function; this allows the smoothing function to potentially work with up to 6 application activities. According to the verification requirements for the Behaviour Classification Engine, within the 6 minutes verification time, application activities will be classified once there are 6 applications being utilised. When the 6 minutes verification time is exceeded, application activities will be processed by the Behaviour Classification Engine even though the total number of activities is less than 6. In comparison with the configuration for scenario C, the setting for scenario D provides the opportunity to improve user convenience when they request access for a protected application when the current SS level does not meet the security requirement.

The simulation results for legitimate users and imposters in scenario D are presented in Table 6.8 and Table 6.9 accordingly. Once again, by setting the time period of the degradation function to 60 minutes, the best system for legitimate users' normal, protected and overall application usages were obtained and they are FRR of 7.49%, 78.86% and 11.63% accordingly. By utilising the same configuration for the framework, the system performance for imposters' counterparts are a FAR of 2.5%, 26.73% and 4.05% respectively.

	The probability (%) of a legitimate user being asked by a security question (FRR)		
Degradation function	**Normal applications**	**Protected application**	**Overall (including normal and protected applications)**
1 min	7.97	100	13.58
10 mins	7.85	96.19	13.2
20 mins	7.77	90.71	12.7
30 mins	7.69	87.46	12.42
40 mins	7.58	84.08	12.03
50 mins	7.57	80.76	11.82
60 mins	7.49	78.86	11.63

Table 6.8: Simulation results of scenario D for legitimate users

	The probability (%) of an imposter NOT being asked by a security question (FAR)		
Degradation function	**Normal applications**	**Protected application**	**Overall (including normal and protected applications)**
1 min	2.48	26.73	4.04
10 mins	2.49	26.73	4.04
20 mins	2.49	26.73	4.05
30 mins	2.49	26.73	4.05
40 mins	2.49	26.73	4.05
50 mins	2.5	26.73	4.05
60 mins	2.5	26.73	4.05

Table 6.9: Simulation results of scenario D for imposters

Table 6.10 demonstrates the smoothing function usage's statistics for all scenarios. As scenario A only utilised 1 application for the smoothing function, it has got 100% for the smoothing function utilising 1 application. As the other scenarios employed a maximum number of applications for the smoothing function with 3, 3 and 6 applications respectively, they all had a mixture of smoothing function usage.

Smoothing function	Scenario A	Scenario B	Scenario C	Scenario D
1 application	100%	57.5%	45.13%	44.45%
2 applications	-	32.53%	32.43%	31.51%
3 applications	-	9.97%	22.44%	14.24%
4 applications	-	-	-	6.65%
5 applications	-	-	-	2.21%
6 applications	-	-	-	0.94%

Table 6.10: The statistic on the smoothing function usage for all four scenarios

Table 6.11 presents the statistic on the usage of the "check if there are any applications not being processed before the protected application" clause for each scenario with the degradation function set to 60 minutes. For instance, for legitimate users, there were some cases that applications not being processed before the protected application, and the usage of these protected applications is 6.18% of the total protected application usage for scenario B; despite the initial SS level smaller than 2, 10.26% of this 6.18% protected application usage did not need the legitimate user to answer a randomly selected security question because after processing those unprocessed applications, the current SS level is greater or equal to 2.

	Scenario A	Scenario B	Scenario C	Scenario D
Answer 'yes' to the clause for legitimate users	-	6.18%	6.18%	10.14%
The percentage of saving the legitimate user to answer a security question because of this clause	-	10.26%	5.13%	17.19%
Answer 'yes' to the clause for imposters	-	0.29%	0.29%	0.36%
The percentage of saving the imposter to answer a security question because of this clause	-	0%	0%	0%

Table 6.11: The statistic on the usage of the "check if there are any applications not being processed before the protected application" clause

6.4 Discussion

Based upon the simulation result, it demonstrates that the Behaviour Profiling framework outperforms the PIN based authentication method in several aspects: security, convenience and extra protection on protected applications (high value applications). In order to illustrate this point, the most secure way of deploying a PIN on a mobile device is utilised which requires a PIN after the mobile device has been idle for more than one minute. By utilising this setting, the PIN based method was applied to the same simulation data; it required users to enter a PIN for every single application usage (100% intrusive authentication) regardless the status of the application. Therefore, the PIN based authentication method is not user friendly after all. From a security point of view, people cannot rely on the PIN based authentication technique as their weakness was well demonstrated in Chapter 2 section 2.4.1. To compare with the PIN based authentication technique performance, the results of simulation scenario A is used because the way that how scenario A simulates is the most closed set up to how the PIN based method operates. As demonstrated in Table 6.2 and Table 6.3, by utilising 60 minutes for the degradation function, the Behaviour Profiling framework achieved the best system performance with an overall FRR of 11.46% and FAR of 4.17%. For the 11.46% of FRR, it indicates that there is a 11.46% of chance that a legitimate user will be challenged by a security question. At the same time, this shows that with 88.54% the chance the legitimate user will be transparently verified through their application activities and automatically obtain access to the device. In addition, the chance for the legitimate user to be transparently verified is boosted to 91.4% (1-8.6%(FRR)) when the legitimate user only requests access for normal applications. Despite the FRR for the protected application being significantly higher in comparison with the normal applications' counterpart, the legitimate user still has a 25.2% chance to access the protected application without needing answering a randomly selected security question. In addition, the usage of the protected application only represents 4.3% of the

total application usage. This indicates that the legitimate users will be mainly verified transparently. For the 4.17% of FAR, it reveals that the imposter has only got 4.17% of the chance to misuse an application and 95.83% of the time they will be denied access to an application. The 4.3% of overall FAR was obtained by utilising the simulation programme to continuously classify the imposter's data only; the imposter's application usage was permitted even though they could not answer the randomly selected security question. In reality, it is highly likely the imposter will be intrusively prompted with a randomly selected security question; if they fail to answer the question three times in a row, the device will be locked down and they will not be able to access the mobile device anymore. By utilising the same configuration, the chance for an imposter to misuse a normal application is a 4.36% as the opportunity for them to abuse the protected application is none. This demonstrates that in comparison with the PIN based authentication technique, by utilising the Behaviour Profiling framework, the chance for the imposter to abuse the mobile device is minimised and extra protection is offered to high value applications. Based upon the above discussion, it suggest that the Behaviour Profiling framework is capable of providing continuous and transparent protection (for the majority of the time) for mobile devices by utilising user application activities and it outperforms the PIN based authentication technique in the areas of security and user convenience.

The impact of the smoothing function and verification time were examined through the simulation scenarios. As demonstrated by the simulation results (from Table 6.2 to Table 6.9), the best system performance (11.24% for overall FRR and 4.09% for overall FAR) was obtained by utilising a combination of the smoothing function of 3 applications and the verification time of 3 minutes. With the other configuration of the smoothing function and settings of the verification time, the overall system performance decreased slightly.

The effectiveness of the degradation function was also evaluated by the simulation. As illustrated by the simulation results (form Table 6.2 to Table 6.9), when the time period of the degradation function gets longer, the FRR reduces which allows the legitimate users to gain access more easily. On the other hand, the impact on the FAR is not significant due to the imposter's activities were verified in a continuous fashion and hence most of the imposters experienced a negative SS value which the degradation function has no influence on. However, in real life, an imposter could pick up a mobile device with a high SS level if the time period was set too long and the device was left with a high level SS initially. This would increase the chance for the imposter to abuse both the normal and protected applications.

As demonstrated by Table 6.11, by utilising the "check if there are any applications not being processed before the protected application" clause, a small portion of the access request on the protected applications was automatically permitted to legitimate users and this improves user convenience. However, none of the imposter's activities on the protected applications were bypassed by utilising the same clause. This may be caused by the imposter's activities that were classified in a continuous manner and hence the chance for an imposter to get a positive SS level is relative small.

6.5 Conclusion

The simulation results demonstrate that the Behaviour Profiling framework outperforms the PIN based authentication technique in terms of security and user convenience. By utilising the smoothing function of three applications, verification time of 3 minutes and a 60 minute time period of the degradation function, the Behaviour Profiling framework achieved the best performance with FRR rates of 7.57%, 77% and 11.24% for the normal, protected and overall applications accordingly and with FAR rates of 3.42%, 15.29% and 4.09% for their counterparts. It is clearly from these results, that the Behaviour Profiling framework is able to provide continuous and transparent verification to protect mobile devices and the research project makes a valuable contribution to the area of mobile security.

7 Conclusions and Future Work

This chapter summaries the thesis by reviewing the project's main achievements and discussing the project's limitations. The chapter then highlights the future research directions within the mobile device security field.

7.1 Achievements of the research

Overall, the project has achieved all the objectives initially set out in Chapter 1, with a series of experimental studies and simulations undertaken for the development of a behaviour profiling technique. The full achievements are:

1. A thorough investigation of the current security challenges that mobile devices experience (Chapter 2). By reviewing the complex environment that mobile devices operate in, the sensitive information that they possess, the numerous security threats that lead to misuse and the lack of protection that is offered, the need for a robust security mechanism which can offer continuous protection is identified.
2. A comprehensive review of biometric authentication techniques (Chapter 3). By presenting a solid background for biometric authentication mechanisms, focus was then given for those which have the potential of providing security on mobile devices. Contributions of previous behavioural related mobile security projects (both authentication (host based) and IDS (network based)) have been studied, determining the scope and requirement for studying the feasibility of utilising a behaviour profiling technique within the mobile host environment.
3. An experimental investigation and evaluation of the behaviour profiling technique through mobile user application activities (Chapter 4). A series of experimental studies were conducted on real user application usages from the MIT Reality dataset. Firstly, by utilising the descriptive statistical method, several application features demonstrated the potential for a successful behaviour profiling classification. This was then evaluated by employing more complex solutions (i.e. Neural Networks and a rule based approach) for a preliminary study; more importantly, the study demonstrated the most optimal classifier (i.e. the rule based approach) to behaviour profiling within the mobile host environment. The feasibility of the behavioural profiling technique was investigated on mobile users' intra-standard applications, telephony, text message and multi-instance applications, utilising a combination of the rule based approach, a dynamic profiling technique and a smoothing

function. In comparison with other biometric techniques, the result of the investigation is within a level of acceptance. This successfully demonstrates the behaviour profiling technique's potential to verify mobile user via their application usages.

4. The proposal and completion of a novel mobile security verification framework by utilising the behaviour profiling technique (Chapter 5). The proposed architecture continuously verifies user application usage based upon three criteria: the smoothing function (for improving performance), the verification time (for ensuring security within certain timeframes) and the application nature (offering better convenience). By utilising the verification result, a dynamic contribution towards current SS level is allocated depending upon individual users and applications. The SS level adds a layer of intelligence to the verification process, providing the possibility level presenting how secure the mobile device is rather than one-off pass or fail verification for the user's identity. With high level system security, automatic access will be granted to users; while, with low level system security, users would have to verify themselves through a knowledge based approach before they can access the device. The proposed framework was also designed to collaborate with other security controls (i.e. authentication and IDS systems) for providing enhanced mobile security.
5. The evaluation of the Behaviour Profiling framework via a simulation approach (Chapter 6). A number of configurations of the proposed framework were evaluated by utilising the MIT Reality dataset. System performance was calculated for both legitimate users and imposters based up their application usage. By utilising the smoothing function of three applications, verification time of 3 minutes and a time period of 60 minutes of the degradation function, the Behaviour Profiling framework obtained the best performance with FRR rates of 7.57%, 77% and 11.24% for the normal, protected and overall applications respectively and with FAR rates of 3.42%, 15.29% and 4.09% for their counterparts.

A number of papers related to the research project have been presented and published in refereed journal and conferences (the papers are demonstrated in Appendix (F)). In particular, the author was awarded a best PhD paper prize at the 10th European Conference on Information Warfare and Security (ECIW). As a result, it is deemed that the research has made positive contributions to the mobile security domain, and especially in the field of biometric verification.

7.2 Limitations of the research project

Despite the research objectives having been met, a number of limitations associated with the project can be identified. The key limitations of the research are summarised below.

1. The MIT Reality dataset was collected during the period of 2004 -2005. At that time, the number of applications available to users to choose was limited; this resulted in a large similarity of intra-standard application usage between mobile users and hence increased difficulty for any classification methods. Also, the dataset only contained two intra-extended applications' (i.e. telephony and text message) activities; although other intra-extended applications (e.g. web browsing) were utilised by users the logging software was not designed to collect the extra unique information (e.g. web address) from those intra-extended applications. Having said this, the experiment was able to utilise the MIT dataset to demonstrate that the intra-extended application contains far more discriminate information than the intra-standard application does.
2. In order to maximise the number of participants, the experiment dataset only contained one month of overlapping user activities. As a result, the performance of the behaviour profiling technique was not examined by utilising a longer profile period despite the experimental results of Chapter 4 suggesting that the longer the profiling period is, the better the performance would be.
3. The chosen one month dataset contains a large amount of information (more than 45,000 application activities) and it requires significant amount of computer resource to be processed within the Matlab environment. This limitation restrains computational greedy classifiers (e.g. RBF neural network) to be employed on the full one month dataset but a small proportion of activities extracted from the one month dataset. Therefore, the best theoretical performance for a behaviour profile technique was arguably unable to be obtained although none of current mobile devices would be capable of accommodating such a classifier.
4. Due to limited resources that were available, only the core functions of the standalone mode of the Behaviour Profiling framework were evaluated through the developed simulation system, but the performance for the dependent mode of the Behaviour Profiling framework (i.e. collaboratively working with an authentication or IDS system) was un-examined. Given the successful investigation of the standalone mode of the Behaviour Profiling framework, it was deemed that when the Behaviour Profiling framework

operates in dependent mode, it would arguably make a positive contribution towards the overall performance of an authentication or IDS system.

7.3 Suggestions & Scope for Future Work

This research project has improved the domain of end user verification for mobile devices. Nonetheless, there are a number of areas in which future work could be carried out to advance upon what has been achieved in this research. The details of future work are listed below:

1. Design a universal application collection software package. This would meet the first requirement allowing the Behaviour Profiling framework to be deployed on real mobile devices. It will be necessary that the application collection software has a small footprint without any substantial degradation of mobile system performance.
2. Development of a Behaviour Profiling Framework prototype on real mobile devices. This would allow a comprehensive evaluation of the behaviour profiling technique on live user application interactions to be proceeded and real participant feedbacks to be collected.
3. Research in identifying positive application features. It is evidenced by the Chapter 4 experiments that positive application features can improve the classification result while other application features will downgrade the classification result and also consume more computational power. By examining the uniqueness of intra-extended applications features, such as the web address for a web service, the performance of the behaviour profiling technique could be arguably improved. Therefore, the process of identifying positive features is mission critical for a wider deployment of the behaviour profiling technique.
4. Further research and development of the dependent working mode of the Behaviour Profiling framework. In particular, cooperating with the TAS authentication system or the KBTA IDS architecture within the mobile host environment. Then, it is envisaged that the performance of the TAS system will be improved in a number of scenarios, such as when a user composes a text message, the user's identity is verified based upon their keystroke activities (i.e. original TAS setting) and also to whom and where the message is compiled (i.e. the behaviour profiling technique). The KBTA architecture will also benefit from the behaviour profiling technique, as it will not only be able to detect mobile malware but also user related misuse.
5. Further investigation of the data storage for the Behaviour Profiling framework. As the simulation system was implemented on a normal PC, data storage was never an issue.

However, the storage space in where the Behaviour Profiling framework will occupy should be taken into consideration when implementing the framework on a mobile device. Whilst it is not envisaged to be a particular problem, given the storage of all application usage, issues within regards to data retention and privacy need to be considered.

7.4 The Future of Verification for Mobile Devices

The popularity and development of mobile devices increase significantly year after year. People rely on their devices to complete personal and business tasks on a daily basis, from storing private information to accessing corporate emails, from paying goods at superstores to connecting corporate networks. It is highly likely that these activities involve a certain degree of sensitive and confidential information. As more mobile services are being developed and mobile hardware capability is being enhanced, such a trend will continue to exist. However, the potential damage associated to the device is also magnified should the device be misused. It can be deemed that at this point the need for verifying a user's identity is more essential than ever before.

Despite many controls that are currently being utilised for verifying users' identity and detecting device misuse, this project has emphasised the need for a robust and reliable security mechanism which should operate in a continuous and transparent manner to offer both the security and user convenience. To this end, this research project has designed and developed a host based novel Behaviour Profiling framework capable of providing continuous and user friendly verification of the user in its own right or collaborating with other security controls (e.g. TAS or KBTA) to offer enhanced security.

To conclude, verifying a mobile user's identity will be crucial in the near future due to the financial services the mobile device provides and the sensitive information it carries. It is envisaged these services and information could become the main motivation towards device misuse. In order to provide adequate protection on mobile devices, mechanisms will have to utilise multiple security techniques and operate in a continuous and user friendly fashion.

References

1. Acuity Market Intelligence (2009) "The Future of Biometrics Market Research Report", available at: http://www.acuity-mi.com/FOB_Report.php, date accessed: 24/06/2011
2. Advancedsourcecode (2011) "Coherent Point Drift for Biometric Identification", available at: http://www.advancedsourcecode.com/earrecognition.asp, date accessed: 29/07/2011
3. Al-Baker, O., Benlamri, R. and Al-Qayedi, A. (2005) "A GPRS based remote human face identification system for handheld devices", In *Second IFIP International Conference on Wireless and Optical Communications Networks*, pages 367– 371, 2005.
4. Anderson, J.P. (1980) "*Computer Security Threat Monitoring and Surveillance*", available at: http://seclab.cs.ucdavis.edu/projects/history/papers/ande80.pdf, date accessed: 26 November 2007
5. Androlib (2011) "ccumulated number of Application and Games in the Android Market", available from: http://www.androlib.com/appstats.aspx, date accessed: 22 September 2011
6. Aol Tech (2011) "Orange and Barclaycard launch 'Quick Tap' NFC mobile payments in the UK", available at: http://www.engadget.com/2011/05/20/orange-and-barclaycard-launch-quick-tap-nfc-mobile-payments-in/, date accessed: 22/07/2011
7. Apple Inc (2011) "Apple's App Store Downloads Top 15 Billion", available from: http://www.apple.com/pr/library/2011/07/07Apples-App-Store-Downloads-Top-15-Billion.html, date accessed: 23/08/2011
8. Article Alley (2010) "Bluetooth vs SMS Mobile Phone Marketing", available at: http://www.articlealley.com/article_1750772_3.html, date accessed: 01/05/2011
9. A.T.R. Systems (2003) "Product Listing", available at:http://www.handpunch.com/, date accessed: 11/06/2011
10. Aviv, A.J., Gibson, K., Mossop, E., Blaze, M. and Smith, J.M. (2010) "Smudge Attacks on Smartphone Touch Screens", Proceeding in WOOT'10 Proceedings of the 4th USENIX conference on Offensive technologies.
11. AxxonSoft (2011) "Face Recognition", available at: http://www.axxonsoft.com/ integrated _security_solutions/face_recognition/index.php?phrase_id=3032106, date accessed: 09/06/2011
12. BBC (2004) "First mobile phone virus created", available at: http://news.bbc.co.uk/ 1/hi/technology/3809855.stm, access date: 30 March 2011.

13. BBC news (2007) “Switch on for Square Mile wi-fi”, available at: http://news.bbc.co.uk/1/hi/technology/6577307.stm, date accessed: 01/05/2011
14. BBC (2008) “’60,000’ devices left in cabs”, available at: http://news.bbc.co.uk/1/hi/7620569.stm, date accessed: 29 March 2009.
15. BBC news (2009) “Mobile phone ID fraud increases”, available at: http://news.bbc.co.uk/newsbeat/hi/technology/newsid_8242000/8242709.stm, date accessed: 07/05/2011
16. BBC news (2010) “Users complacent about mobile security, finds research”, available at: http://www.bbc.co.uk/news/technology-11634069, date accessed: 06/05/2011
17. BBC (2011) “Orange customers of Everything Everywhere get mobile payments”, available at: http://www.bbc.co.uk/news/technology-12287009, date accessed: 21/07/2011
18. Berg Insight (2011) “Berg Insight predicts 709 million mobile money users in emerging markets by 2015”, available at: http://www.berginsight.com/News.aspx?m_m=6&s_m=1, date accessed: 16/062011
19. Bhattacharyya, D., Ranjan, R., Alisherov, A.F. and Choi, M. (2009) “Biometric Authentication: A Review” International Journal of u- and e- Service, Science and Technology Vol. 2, No. 3, September, 2009
20. BioPassword (2007) “*Keystroke dynamics science and technology from* BioPassword*”,* available from: http://www.biopassword.com/keystroke-dynamics-science.php, date accessed: 24/11/2007
21. Biometric Newsportal (2011) “Retina biometrics”, available at: http://www.biometricnewsportal.com/retina_biometrics.asp, date accessed: 20/05/2011
22. Bio-metrica (2011) “Classifications / Type of biometrics”, available at: http://www.bio-metrica.com/RC_KC_BT2.php, date accessed: 29/07/2011
23. Bledsoe, W. W. (1966) “Man-Machine Facial Recognition: Report on a Large-Scale Experiment”, Technical Report PRI 22, Panoramic Research, Inc., Palo Alto, California.
24. Bluetooth SIG (2011) “Career Opportunities at the Bluetooth SIG”, available at: https://www.bluetooth.org/About/career.htm, date accessed: 28/03/2011
25. Brightsideofnews (2011) “How to Create a Safe Password”, available at: http://www.brightsideofnews.com/news/2011/6/1/how-to-create-a-safe-password.aspx, date accessed: 29/07/2011
26. Bromba (2011) “Fingerprint Cellphone”, available at: http://www.bromba.com/protoe.htm#Handy, date accessed: 01/06/2011

27. Browning, D. and Kessler, G.C. (2009) “Bluetooth Hacking: A Case Study”, *Journal of Digital Forensics, Security and Law*, Vol.*4* (2), pp.57-71.

28. BTopenzone (2011) “What's a Wi-Fi hotspot?”, available at: http://www.btopenzone.com /help/whats-a-hotspot/index.jsp, date accessed: 15/06/2011

29. Buennemeyer, T.K., Nelson, T.M., Clagett, L.M., Dunning, J.P., Marchany, R.C. and Tront, J.G. (2008) “Mobile device profiling and intrusion detection using smart batteries”, Proceedings of the 41st Hawaii International Conference on System Sciences, pp.296–296.

30. Burge, M. and Burger, W. (2000) "Ear biometrics in computer vision," *Pattern Recognition, 2000. Proceedings of 15th International Conference on* Pattern Recognition, vol.2, pp.822-826, doi: 10.1109/ICPR.2000.906202, URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=906202&isnumber=19583

31. Buchoux, A. and Clarke N.L. (2008) “Deployment of Keystroke Analysis on a Smartphone”, Proceedings of the 6th Australian Information Security & Management Conference, 1-3 December, Perth, Australia

32. Cabume (2011) “Wi-Fi use doubles as mobile broadband increasingly sidelined”, available at: http://www.cabume.co.uk/hardware/wi-fi-use-doubles-as-mobile-broadband-increasingly-sidelined.html, date accessed: 18/07/2011

33. Campbell, J. P. (1997) “Speaker Recognition: A Tutorial”, Proceedings of the IEEE, volume 85, No. 9, September 1997, pp.1437-1462.

34. Campisi, P., Maiorana, E., Bosco, M.L. and Neri, A. (2009) "User authentication using keystroke dynamics for cellular phones", IET Signal Processing, Vol.3 No.4 pp. 333-341.

35. Canalys (2011) “Google’s Android becomes the world’s leading smart phone platform”, available at: http://www.canalys.com/pr/2011/r2011013.html, date accessed: 03/05/2011

36. Canvas Solutions (2011) “Can I capture signatures on my mobile device using Canvas?”, available at: http://www.gocanvas.com/content/faq/post/can-i-capture-signatures-with-canvas, date accessed: 16/08/2011

37. Cert (2011) “2011 CYBERSECURITY WATCH SURVEY: ORGANIZATIONS NEED MORE SKILLED CYBER PROFESSIONALS TO STAY SECURE”, available at: www.cert.org/archive/pdf/CyberSecuritySurvey2011.pdf, date accessed: 22/06/2011

38. CFCA (2009) “COMMUNICATIONS FRAUD CONTROL ASSOCIATION (CFCA) ANNOUNCES RESULTS OF WORLDWIDE TELECOM FRAUD SURVEY”, available at: http://www.cfca.org /pdf/survey/2009%20Global%20Fraud%20Loss%20Survey-Press%20Release.pdf, date accessed: 08/05/2011

39. Chang, K., Bowyer, K.W., Sarkar, S. and Victor, B. (2003) “Comparison and combination of ear and face images in appearance-based biometrics”, IEEE Trans. PAMI, vol. 25, no. 9, pp. 1160–1165.
40. Clarke, N. (2004) “Advanced User Authentication for Mobile Devices”, PhD thesis.
41. Clarke, N. (2011) “Transparent User Authentication”, Springer, ISBN 978-0-85729-804-1
42. Clarke, N.L. and Furnell, S.M. (2005) “Authentication of users on mobile telephones - A survey of attitudes and practices”, Computers & Security, vol. 24, no. 7, pp519-527
43. Clarke, N.L. and Furnell, S.M. (2006) “Authenticating Mobile Phone Users Using Keystroke Analysis”, International Journal of Information Security, ISSN:1615-5262, pp.1-14.
44. Clarke, N.L and Mekala, A.R. (2007) “The application of signature recognition to transparent handwriting verification for mobile devices”, Information Management & Computer Security, volume 15, issue 3, pp214-225.
45. Clarke, N.L., Karatzouni, S., and Furnell, S.M. (2008) “Transparent Facial Recognition for Mobile Devices”, Proceedings of the 7th Security Conference, Las Vegas, USA, 2nd-3rd June, 2008
46. Clevelandtime (2011) “Hand Punch Biometric Time Clock”, available at: http://www.clevelandtime.com/handpunch.html, date accessed: 29/07/2011
47. CNET news (2010) “Apple iPhone 4 sales: 1.7 million in three days”, available at: http://news.cnet.com/8301-13579_3-20008980-37.html, date accessed: 28/03/2011
48. Communications Today (2010) “Average Revenue from GSM users declines 8.6 percent”, available at: http://www.communicationstoday.co.in/news-selection/average-revenue-from-gsm-users-declines-8.6-percent-2782-145.html, date accessed: 08/05/2011
49. Communities Dominate Brands (2010) “Lets Understand the Mobile Phone Market, installed base and smartphones vs dumbphones”, available at: http://communities-dominate.blogs.com/brands/2010/12/lets-understand-the-mobile-phone-market-installed-base-and-smartphones-vs-dumbphones.html, date accessed: 28/03/2011
50. ComputerWeekly, (2010) “Millions download suspicious Android wallpaper”, available at: http://www.computerweekly.com/Articles/2010/08/24/242169/Millions-download-suspicious-Android-wallpaper.htm, date accessed: 31 March 2011
51. Covavisaruch, N., Prateepamornkul, P., Ruchikachorn, P. and Taksaphan, P. (2005) “Personal verification and identification using hand geometry”, ECTI Transactions on Computer and Information Technology Vol. 1, no. 2, pp.134–139.

52. Credant (2009) “Phone Data makes 4.2 Million* Brits Vulnerable to ID Theft”, available at: http://www.credant.com/news-a-events/press-releases/337-phone-data-makes-42-million-brits-vulnerable-to-id-theft-.html, date accessed: 14/06/2011
53. Credant (2011) “The Insider threat”, available at: http://www.infosecurity-magazine.com/_virtual/article-downloads/Insider-Threat-WP-0511W.PDF, date accessed: 23/06/201
54. CSO online, 2011 “McAfee confirms Android as favourite mobile target”, available at: http://www.cso.com.au/article/404655/mcafee_confirms_android_favourite_mobile_target/#closeme, date accessed: 12/11/2011
55. Das, R., (2007) “Signature recognition: An introduction to signature recognition as a biometric technology”, Keesing Journal of Documents & Identity, issue 24, pp. 13-14.
56. Daugman, J. (1993) "High confidence visual recognition of persons by a test of statistical independence", *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 15(11), pp. 1148-1161.
57. Derawi, M.O., Nickel, C., Bours, P., and Busch, C. (2010) "Unobtrusive User-Authentication on Mobile Phones Using Biometric Gait Recognition," Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2010
58. Distimo (2010) “Our Presentation From Mobile World Congres 2010 – Mobile Application Stores State Of Play”, [online], http://blog.distimo.com/2010_02_our-presentation-from-mobile-world-congres-2010-mobile-application-stores-state-of-play/, date accessed: 17/01/2011
59. Du, Y. (2006) "*Review of iris recognition*: *cameras, systems, and their applications*", Sensor Review, Vol. 26, Iss: 1, pp.66 – 69.
60. Duta, N. (2009) “A survey of biometric technology based on hand shape”, Pattern Recognition, Vol 42, Issue 11, November 2009, pp.2797-2806.
61. EPIC (2005) “Biometric Comparison Guide”, available at: http://epic.org/privacy/surveillance/spotlight/1005/irid_guide.pdf, date accessed: 19/05/2011
62. Ernst, R. H. (1971) “Hand ID system", US Patent No. 3576537, 1971.
63. Etemad, K. and Chellappa, R. (1997) “Discriminant Analysis for Recognition of Human Face Images”, Journal of the Optical Society of America A, Vol. 14, No. 8, pp. 1724-1733, August 1997.
64. EyeNetWatch (2011) “Biometric Security Solutions”, available at: http://www.eyenetwatch.com/, date accessed: 11/06/2011

65. Face-rec (2011) “Vendors”, available at: http://www.face-rec.org/vendors/, date accessed: 19/05/2011

66. FBI (2010) “Smishing and Vishing”, available at: http://www.fbi.gov/news/stories/2010/november/cyber_112410/cyber_112410, date accessed: 11 April 2011.

67. Fong, A.C.M. and Fong, B. (2008) "Palmprint Alignment for Consumer Applications," *Consumer Electronics, 2008. ICCE 2008. Digest of Technical Papers. International Conference on*, pp.1-2, 9-13 Jan. 2008

68. Free-press-release (2011) “Facial Recognition - Emerging as the Fastest Growing Segment”, available at: http://www.free-press-release.com/news-facial-recognition-emerging-as-the-fastest-growing-segment-1295508190.html, date accessed: 10/06/2011

69. Fu, K.S., Pyung June Min and Li, T.J. (1970) "Feature Selection in Pattern Recognition", *Systems Science and Cybernetics, IEEE Transactions on* Systems Science and Cybernetics, vol.6, no.1, pp.33-39, doi: 10.1109/TSSC.1970.300326, URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4082284&isnumber=4082276

70. Furnell, S. and Evangelatos, K. (2007) “Public awareness and perceptions of biometrics”, Computer Fraud and Security, vol. 2007, issue 1, pp. 8-13.

71. Furnell, S., Rodwell, P. and Reynolds, P. (2001) “A Conceptual Security Framework to Support Continuous Subscriber Authentication in Third Generation Networks”, Proceedings of Euromedia 2001.

72. F-Secure (2005) “F-Secure first to launch Mobile Anti-Virus for the retail market”, available at: http://www.f-secure.com/en_HK/about-us/pressroom/news/2005/fs_news_20050802_2_eng.html, date accessed: 13/04/2011

73. Gartner (2009) “Gartner Identifies the Top 10 Consumer Mobile Applications for 2012”, available at: http://www.gartner.com/it/page.jsp?id=1230413, date accessed: 03/05/2011

74. Geekosystem (2011) “Facebook Will Go Ahead and Scan Your Face Now”, available at: http://www.geekosystem.com/facebook-face-recognition/, date accessed: 29/07/2011

75. GigaOM (2011) “Mobile devices overtake computers on Wi-Fi networks”, available at: http://gigaom.com/2011/06/21/mobile-devices-overtake-computers-on-wi-fi-networks/, date accessed: 18/07/2011

76. GlobalSecurity (2011) “Biometrics”, available at: http://www.globalsecurity.org/security/systems/biometrics.htm, date accessed: 10/09/2011

77. Goldstein, A.J., Harmon, L.D., and Lesk, A.B. (1971) “Identification of Human Faces”, proceeding of IEEE, Vol, 59, No. 5, pp.748-760, May 1971.

78. Goode Intelligence (2010) “mSecurity Survey 2010 Report”, available at: http://www.goodeintelligence.com/report-store/view/msecurity-survey-2010-report, date accessed: 08/05/2011
79. Gosset, P. (1998) “ASPeCT: Fraud Detection Concepts: Final Report”, Doc Ref. AC095/VOD/W22/DS/P/18/1
80. GSA (2011a) “GSM/3G and LTE Market Update”, available at: http://www.gsacom.com/downloads/pdf/GSA_GSM_3G_and_LTE_market_update_030311.php4, date accessed: 27/03/2011
81. GSA (2011b) “GSM/3G Stats”, available at: http://www.gsacom.com/news/statistics.php4, date accessed: 27/03/ 2011
82. GSM World (2009) “Market data summary”, available at: http://www.gsmworld.com/newsroom/market-data/market_data_summary.htm, date accessed: 26 March 2011
83. GSM World (2011) “Home of the GSM association”, available at: http://www.gsmworld.com/index.htm, date accessed: 23 March 2011.
84. Helium (2008) “How a lost or stolen cell phone can lead to identity theft”, available at: http://www.helium.com/items/1161605-how-a-lost-or-stolen-cell-phone-can-lead-to-identity-theft, accessed date: 18 April 2011
85. Henry, E. (1900) *Classification and Uses of Finger Prints*, Routledge, London, 1900. Available at: http://galton.org/fingerprints/books/henry/henry-classification.pdf, date accessed: 17/05/2011
86. Iannarelli, A. (1989) “Ear Identification”, Forensic Identification Series, Paramont Publishing Company, Fremont, Califomia, 1989
87. Indiamart (2011) “Usb Fingerprint Reader”, available at: http://www.indiamart.com/softlinkasia pvltd/services.html, date accessed: 29/07/2011
88. International Biometric Group (2009) “IBG's Biometrics Market and Industry Report 2009-2014”, available at: http://www.ibgweb.com/products/reports/bmir-2009-2014, date accessed: 01/06/2011
89. Intomobile (2010) “BlackBerry App Usage Beats iPhone’s During Workday – Research”, available at: http://www.intomobile.com/2010/04/14/blackberry-app-usage-beats-iphones-during-workday-research/, date accessed: 01/08/2011
90. Itimes (2010) “Retinal Scan & Applications”, available at: http://www.itimes.com/public/people/iti133802/blog/Retinal-Scan-Applications, date accessed: 29/07/2011

91. Jain, A.K., Duin, R.P.W. and Jianchang Mao (2000) "Statistical pattern recognition: a review", *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, vol.22, no.1, pp.4-37, doi: 10.1109/34.824819, URL: http://ieeexplore.ieee.org/stamp/stamp.jsp ?tp=&arnumber=824819&isnumber=17859

92. Jain, A. K., Ross, A. and Pankanti, S. (1999) "A Prototype Hand Geometry-based Verfication System," 2nd International Conference on Audioand Video-based Biometric Person Authentication, pp. 166-171.

93. Jain, A.K., Ross, A. and Prabhakar, S. (2004), "An introduction to biometric recognition," *Circuits and Systems for Video Technology, IEEE Transactions on Circuits and Systems for Video Technology* , vol.14, no.1, pp. 4-20, doi:10.1109/TCSVT.2003.818349

94. Java (2011) "Learn about Java Technology", available at: http://www.java.com/en/about/, date accessed: 22/06/2011

95. JiWire (2009) "JiWire Mobile Audience Insights Reports", available at http://www.jiwire.com/downloads/pdf/JiWire_MobileAudienceInsights_Q409.pdf, date accessed: 18/07/2011

96. Juniper Research (2010) "A world of Apps", available at: http://www.juniperresearch.com /shop/products/whitepaper/pdf/MAS10_White%20Paper.pdf, date accessed: 28/03/2011

97. Karatzouni, S., Clarke, N.L., and Furnell, S.M. (2007) "NICA design specification. University of Plymouth. Available at: http://www.cscan.org/nica/. Accessed 10 Apr 2011

98. Khan, S. and Gurkas, P. (2010) "Identification Using Biometric Technology: Issues And Attitudes", Proceeding of IADIS International Conference on ICT, Society and Human Beings 2010, Freiburg, July 28-31, 2010, pp.27-34.

99. Knowyourmobile (2011) "NFC payments to provide $50 billion revenue by 2014", available at: http://www.knowyourmobile.com/blog/932946/nfc_payments_to_provide_50_ billion _revenue_by_2014.html, date accessed: 21/07/2011

100. Kong, A., Zhang, D. and Kamel, M. (2009) "A survey of palmprint recognition", Pattern Recognition, Volume 42, Issue 7, July 2009, pp.1408-1418.

101. Kothavale, M., Markworth, R., and Sandhu, P. (2004) "Computer Security SS3: Biometric Authentication", available at: http://www.cs.bham.ac.uk/~mdr/teaching/ modules03/security/students/SS3/handout/index.html, date accessed: 29/07/2011

102. Kaspersky Lab (2011a) "European Users Mobile Behaviour and Awareness of Mobile Threats", available at: http://www.kaspersky.com/news?id=207576289, date accessed: 14/06/2011

103. Kaspersky Lab (2011b) “Mobile Threats Double in Number”, available at: “http://www.kaspersky.co.uk/news?id=207576301”, date accessed: 14/06/2011

104. Kurkovsky, S. and Syta, E. (2010) “Digital natives and mobile phones: A survey of practices and attitudes about privacy and security”, In Proceedings of the 2010 IEEE International Symposium on Technology and Society (ISTAS), pp. 441-449.

105. Lu, J. and Zhang, E. (2007) "Gait recognition for human identification based on ICA and fuzzy SVM through multiple views fusion", Pattern Recognition Letters, Vol. 28, pp. 2401–2411, 2007.

106. Maclin, S (2008) “Interesting Facts About Cell Phones”, available at: http://usacellsearch.com /tag/hexagonal-cells/, date accessed: 10 February 2009

107. Mainguet, J (2011) “Cellphones / PDAs / GPS ”, available at: http://fingerchip.pagesperso-orange.fr/biometrics/types/fingerprint_products_pdaphones.htm, date accessed: 01/06/2011

108. Marketsandmarkets (2011) “Global Biometrics Technology Market (2010-2015) – Market Forecast by Products, End-User Application and Geography”, available at: http://www.marketsandmarkets.com/Market-Reports/biometric-market-278.html, date accessed: 05/05/2011

109. Martin, T., Hsiao, M., Ha, D. and Krishnaswami, J. (2004) “Denial-of-Service Attacks on Battery-powered Mobile Computers”, Second IEEE International Conference on Pervasive Computing and Communications, pp. 309-318, IEEE Computer Society, Washington, DC, USA

110. McAfee (2010) “McAfee Threats Report: Fourth Quarter 2010”, available at: https://secure.mcafee.com/us/resources/reports/rp-quarterly-threat-q4-2010.pdf, date accessed: 30/03/2011

111. McAfee (2011a) “Massive Phishing Attacks Strike Bank of China Users”, available at: http://blogs.mcafee.com/mcafee-labs/massive-online-bank-phishing-attacks-in-china, date accessed: 11/04/2011

112. Mcafee (2011b) “Mobility and Security: Dazzling Opportunities, Profound Challenges”, available at: http://www.mcafee.com/us/resources/reports/rp-cylab-mobile-security.pdf, date accessed: 13/06/2011

113. Metropolitan Police Service (2011) “Safeguarding your mobile phone”, available at: http://www.met.police.uk/crimeprevention/phone.htm, date accessed: 29/03/2011

114. Miettinen, M., Halonen, P. & Hatonen, K. (2006) Host-based intrusion detection for advanced mobile devices. In *proceedings of the 20th International Conference on Advanced Information Networking and Applications (AINA' 06)* (pp.72-76). IEEE Computer Society Washington, DC, USA

115. Mobilecommercedaily (2010) "50M NFC-enabled mobile devices to hit the market in 2011: Inside Contactless", available at: http://www.mobilecommercedaily.com /2010/11/30/50m-nfc-enabled-mobile-devices-to-hit-the-market-in-2011-inside-contactless, date accessed: 15/06/2011

116. Moody, J. (2004) "Public perceptions of biometric devices: the effect of misinformation on acceptance and use", Journal of Issues in Informing Science and Information Technology, vol.1, pp. 753-761.

117. Muir, J (2003) "*Decoding Mobile Device Security*", available at: http://www.computerworld .com /securitytopics/security/story/0,10801,82890,00.html, date accessed: 12/04/2011

118. Neruotechnology (2011) "VeriFinger", available at: http://www.neurotechnology.com /verifinger.html, date accessed: 24 November 2011

119. Newbusiness (2010) "Use of mobiles for online transactions grows", available at: http://www.newbusiness.co.uk/articles/telecommunications/use-mobiles-online-transactions-grows, date accessed: 21/07/2011

120. Newscientist (2005) "Ear recognition may beat face biometrics", available at: http://www.newscientist.com/article/mg18725095.300-ear-recognition-may-beat-face-biometrics.html, date accessed: 05/05/2011

121. PC advisor (2010) "4G held back by 3G investment", available at: http://mobile.pcadvisor.co.uk/news/mobile-phone/3255565/ofcom-lets-mobile-networks-use-2g-spectrum-for-3g-services/, date accessed: 28 April 2011

122. PCWorld (2006) "McAfee Warns of SMiShing Attacks", available at: http://www. pcworld.com/article/126932/mcafee_warns_of_smishing_attacks.html, date accessed: 11/04/2011

123. PC world (2009) "SuperSpeed USB 3.0: More Details Emerge", available at: http://www. pcworld.com/article/156494/superspeed_usb_30_more_details_emerge.html, date accessed: 28/03/2011

124. Plamondon, R. and Lorette, G. (1989) "Automatic signature verification and writer identification — the state of the art", Pattern Recognition, Volume 22, Issue 2, 1989, pp. 107-131.

125. PolyU (2009) “The Hong Kong Polytechnic University (PolyU) 2D_3D_Palmprint Database”, available at: http://www4.comp.polyu.edu.hk/~biometrics/2D_3D_Palmprint.htm, date accessed: 29/07/2011

126. Ponemon Institute (2011) “2010 Annual Study: U.K. Cost of a Data Breach”, available at: http://www.symantec.com/content/en/us/about/media/pdfs/UK_Ponemon_CODB_2010_031611.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2011Mar_worldwide_costofdatabreach, date accessed: 06/05/2011

127. Prabhakar, S., Pankanti, S. and Jain, A.K. (2003) "Biometric recognition: security and privacy concerns", *Security & Privacy, IEEE*, vol.1, no.2, pp. 33-42, Mar-Apr 2003, doi: 10.1109/MSECP.2003.1193209, URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1193209&isnumber=26759

128. ProtecStar (2009) “ProtectStar™ Mobile Firewall 1.0” available at http://www.protectstar.com/index.php?y=60&x=73, date accessed: 15/01/2009

129. Prokoski, F.J., Riedel, R.B. and Coffin, J.S. (1992) “Identification of Individuals by Means of Facial Thermography”, in Proceedings of the IEEE International Conference on Security Technology, Crime Countermeasures, 1992, pp.120-125, URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=253768&userType=inst

130. Qualcomm (2010) “Qualcomm Ships First Dual-CPU Snapdragon Chipset”, available at: http://www.qualcomm.com/news/releases/2010/06/01/qualcomm-ships-first-dual-cpu-snapdragon-chipset, date accessed: 14 June 2011

131. Queen’s University (2011) “Gait Analysis”, available at: http://me.queensu.ca/People/Deluzio/Gait.html, date accessed: 29/07/2011

132. Regenersis (2009) “Regenersis launches FONEBAK.com allowing consumers to sell their phones for cash, and donate some or all of the proceeds to one of the UK's best loved charities – BBC Children in Need”, available at: http://www.regenersis.com/media-centre/news/2009/oct/6/regenersis-launches-fonebakcom-allowing-consumers-to-sell-their-phones-for-cash-and-donate-some-or-all-of-the-proceeds-to-one-of-the-uks-best-loved-charities--bbc-children-in-need, date accessed: 18 April 2011

133. Robinson, J.A., Liang, V.W., Chambers, J.A.M. and MacKenzie, C.L. (1998) "Computer user verification using login string keystroke dynamics", *Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions on Systems, Man, and Cybernetics*, vol.28, no.2, pp.236-241, Mar 1998
doi: 10.1109/3468.661150

134. Newscientist (2007) “Cellphone firewall” available at: http://www.newscientist.com/blog/invention/2007/04/cellphone-firewall.html, accessed: 14/04/2011

135. NFC Forum (2011) “NFC and Contactless Technologies”, available at http://www.nfc-forum.org/aboutnfc/nfc_and_contactless/, date accessed: 15/11/2011

136. Rao, J.R., Rohatgi, P., Scherzer, H. and Tinguely, S (2002) "*Partitioning Attacks: Or How to Rapidly Clone Some GSM Cards*," IEEE Symposium on Security and Privacy, 2002, *sp*, p. 31

137. Sanchez-Reillo, R. (2000) “Hand Geometry Pattern Recognition Through Gaussian Mixture Modeling,” 15th International Conference on Pattern Recognition, Vol. 2, pp. 937-940.

138. Securelist (2009) “Mobile Malware Evolution: An Overview, Part 3”, available at: http://www.securelist.com/en/analysis?pubid=204792080, date accessed: 30 March 2011

139. Securelist (2011) “Mobile Malware Evolution: An Overview, Part 4”, available at: http://www.securelist.com/en/analysis/204792168/Mobile_Malware_Evolution_An_Overview_Part_4%22, date accessed: 31 March 2011

140. Securitynewsdesk (2011) “Worldwide biometric revenue expected to treble to AED51.4 billion by 2015”, available at: http://www.securitynewsdesk.com/2011/01/21/worldwide-biometric-revenue-expected-to-treble-to-aed51-4-billion-by-2015/, date accessed: 05/05/2011

141. Shu, W. and Zhang, D. (1998) “Automated personal identification by palmprint”, Optical Engineering, vol. 37, no. 8, 1998

142. Sidlauskas, D. P. (1988) “3D hand pro_le identi_cation apparatus", US Patent No. 4736203, 1988.

143. Skyhook (2007) “Resources”, available at: http://www.skyhookwireless.com/developers/wifi.php, date accessed: 15/06/2011

144. Socolinsky, D., Selinger, A. (2004). “Thermal Face Recognition in an Operational Scenario”, Proceedings of CVPR 2004, Washington DC, 27 June-2 July 2004

145. Sola, J. and Sevilla, J. (1997) "Importance of input data normalization for the application of neural networks to complex industrial problems", *Nuclear Science, IEEE Transactions on*, vol.44, no.3, pp.1464-1468, doi: 10.1109/23.589532,
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=589532&isnumber=12840

146. Stajano, F. and Anderson, R (1999) "*The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks*", Proceeding of the 7th International Workshop on Security Protocols, Lecture Notes in Computer Science volume 1796, 1999.

147. Sun, Z., Tan, T., Wang, Y. and Li, S.Z. (2005) "Ordinal palmprint represention for personal identification [represention read representation]", *Computer Vision and Pattern Recognition, 2005. CVPR 2005. IEEE Computer Society Conference on*, vol.1, pp. 279- 284, 20-25 June 2005, doi: 10.1109/CVPR.2005.267

148. Swami, Y. P. and Tschofenig, H (2006) "Protecting mobile devices from TCP flooding attacks", Proceedings of first ACM/IEEE international workshop on Mobility in the evolving internet architecture, pp. 63-68, 2006

149. Telecompaper (2010) "ZigBee's revenue surpasses USD 1 tln", available at: http://www.telecompaper.com/news/zigbees-revenue-surpasses-usd-1-tln, date accessed: 15/06/2011

150. The London Insider (2009) "Lost your phone in a cab? Join the crowd!", available at: http://www.london-insider.co.uk/2009/12/lost-your-phone-in-london-cab/, date accessed: 18 April 2011

151. Times Newspapers (2007) "How quickly did you type that password?", available at: http://technology.timesonline.co.uk/tol/news/tech_and_web/personal_tech/article1667057.ece, date accessed: 24/05/2011

152. TNS mobile life (2011) "The Holistic Portfolio: Decision Making in the Mobile Ecosystem", available at: http://discovermobilelife.com/files/The%20Holistic%20Portfolio%20-%20Decision%20Making%20in%20the%20Mobile%20Ecosystem.pdf, date accessed: 21/06/2011

153. Toshiba America Information Systems (2011) "Face recognition", available at: http://us.toshiba.com/computers/research-center/technology-guides/face-recognition, date accessed: 13/05/2011

154. Trauring, M. (1963) "Automatic comparison of finger ridge patterns", Report No. 190, Hudges Research Laboratories, March 1961, Rev. April 1963

155. Trend Micro (2009) "Trend Micro™ Mobile Security 5.0" available at: http://us.trendmicro.com/us/products/enterprise/mobile-security/index.html, date accessed: 15 January 2009

156. Turk, M.A. and Pentland, A.P. (1991) “Face Recognition Using Eigenfaces”, Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 3-6 June 1991, Maui, Hawaii, USA, pp. 586-591.

157. UKBA (2011) “Using the iris recognition immigration system (IRIS) ”, available at: http://www.ukba.homeoffice.gov.uk/travellingtotheuk/Enteringtheuk/usingiris/, date accessed: 05/05/2011

158. Victor, B., Bowyer, K. and Sarkar, S. (2002) “An evaluation of face and ear biometrics”, in proceeding of ICPR 2002, pp. 429–432.

159. Walesonline (2011) “Internet mobile drive 27% rise in online retails”, available at: http://www.walesonline.co.uk/business-in-wales/business-news/2011/07/19/internet-mobiles-drive-27-rise-in-online-retail-91466-29077062/, date accessed: 21/07/2011

160. Weinstein, E., Ho, P., Heisele, B., Poggio, T., Steele, K. and Agarwal, A. (2002) “Handheld face identification technology in a pervasive computing environment”, In *Pervasive 2002*, pages 48–54, Zurich, Switzerland, 2002.

161. Which? Mobile (2011) “13.5 million UK mobile phone users at risk of fraud”, available at: http://blogs.which.co.uk/mobile/mobile-phones/13-5-million-uk-mobile-phone-users-at-risk-of-fraud/, date accessed: 14/06/2011

162. Which? (2010) “Premium-rate phone fraud costs O2 millions”, available at: http://www.which.co.uk/news/2010/08/premium-rate-phone-fraud-costs-o2-millions-225429/, date accessed: 30 March 2011

163. Wisegeek (2011) “How does a Retinal Scan Work?”, available at: http://www.wisegeek.com/how-does-a-retinal-scan-work.htm, date accessed: 20/05/2011

164. Wiskott, L., Fellous, J.M., Krueuger, N. and Malsburg, C. (1997) “Face Recognition by Elastic Bunch Graph Matching”, IEEE Trans. on Pattern Analysis and Machine Intelligence, Vol. 19, No. 7, pp. 775-779.

165. Wolpert, D.H., Macready, W.G. (1997) "No Free Lunch Theorems for Optimization", *IEEE Transactions on Evolutionary Computation* 1, pp.67-82.

166. Woo, R., Park, A. and Hazen, T. (2006) “The MIT Mobile Device Speaker Verification Corpus: Data collection and preliminary experiments”, Proceeding of Odyssey, The Speaker & Language Recognition Workshop, San Juan, Puerto Rico, June 2006.

167. Wood, H. (1977) “The Use of Passwords for Controlling the Access to Remote Computer Systems and Services”. Computers and Security, Vol.3. C.T. Dinardo, Ed., p.137. Montvale, New Jersey: AFIPS Press.

168. Woodward, J., Orlans, N. and Higgins, P. (2003) “Biometrics. Identity Assurance in the Information Age”. McGraw-Hill.

169. Xu, D., Yan, S., Tao, D., Zhang, L., Li, X., and Zhang, H. (2006) "Human Gait Recognition With Matrix Representation," *Circuits and Systems for Video Technology, IEEE Transactions on Circuits and Systems for Video Technology*", vol.16, no.7, pp.896-903, July 2006, doi: 10.1109/TCSVT.2006.877418

170. Yan, P. and Bowyer, K.W. (2007) “Biometric Recognition Using 3D Ear Shape”, IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE, Vol. 29, No. 8, pp. 1297-1308.

171. Yuan, L. and Mu, Z (2007) "Ear Recognition based on 2D Images," *Biometrics: Theory, Applications, and Systems, 2007, BTAS 2007, First IEEE International Conference on*, pp.1-5.

172. ZDnet (2009) “Smartphones: A bigger target for security threats”, available at:http://www.zdnetasia.com/smartphones-a-bigger-target-for-security-threats-62059391.htm, date accessed: 31 March 2011

173. Zhang, D., Kong, W.K., You, J. and Wong, M. (2003) “Online Palm Print Identification,” *IEEE Trans. Pattern Analysis and Machine Intelligence,* vol. 25, no. 2, pp. 1041-1050, Feb. 2003.

174. ZigBee Alliance (2011) “ZigBee Telecom Services Certified Products ”, available at http://www.zigbee.org/Products/CertifiedProducts/ZigBeeTelecomServices.aspx, date accessed: 15/06/2011

Appendix A: The MIT Reality dataset

Appendix B: The Neural Networks and the rule-based classifiers scripts

Appendix C: The simulation scripts

Appendix D: The preliminary study's experimental results

Appendix E: The final experimental results

Appendix F: Publications

- **Misuse Detection for Mobile Devices Using Behaviour Profiling**
  Li F, Clarke NL, Papadaki M, Dowland PS, International Journal of Cyber Warfare & Terrorism, Volume 1, Issue 1, pp43-55, ISSN: 1947-3435, 2011
- **Behaviour Profiling for Transparent Authentication for Mobile Devices**
  Li F, Clarke NL, Papadaki M, Dowland PS, Proceedings of the 10th European Conference on Information Warfare and Security (ECIW), Tallinn, Estonia 7-8 July, pp307-314, 2011
  Awarded best PhD paper.
- **Behaviour Profiling on Mobile Devices**
  Li F, Clarke NL, Papadaki M, Dowland PS, International Conference on Emerging Security Technologies, 6-8 September, Canterbury, UK, pp77-82, 2010
- **Intrusion Detection System for Mobile Devices: Investigation on Calling Activity**
  Li F, Clarke NL, Papadaki M, Proceedings of the 8th Security Conference, April, Las Vegas, USA, 2009

Misuse Detection for Mobile Devices Using Behaviour Profiling

Fudong Li, Plymouth University, UK

Nathan Clarke and Plymouth University, UK, and Edith Cowan University, Australia

Maria Papadaki, Plymouth University, UK

Paul Dowland, Plymouth University, UK

ABSTRACT

Mobile devices have become essential to modern society; however, as their popularity has grown, so has the requirement to ensure devices remain secure. This paper proposes a behaviour-based profiling technique using a mobile user's application usage to detect abnormal activities. Through operating transparently to the user, the approach offers significant advantages over traditional point-of-entry authentication and can provide continuous protection. The experiment employed the MIT Reality dataset and a total of 45,529 log entries. Four experiments were devised based on an inter-application dataset containing the general application; two intra-application datasets combined with telephony and text message data; and a combined dataset that included both inter-application and intra-application. Based on the experiments, a user's profile was built using either static or dynamic profiles and the best experimental results for the application-level applications, telephone, text message, and multi-instance applications were an EER (Equal Error Rate) of 13.5%, 5.4%, 2.2%, and 10%, respectively.

Keywords: *Applications, Behaviour Profiling, Misuse, Mobile Device, Transparent Authentication*

1. INTRODUCTION

With more than 5 billion users globally, mobile devices have become ubiquitous in our daily life. The modern mobile handheld device is capable of providing many services through a wide range of applications over multiple networks as well as on the handheld itself, such as: voice calling through service provider's network, Internet surfing via Wi-Fi hotspots, video conferencing through a 3G connection, road navigating by GPS (Global Positioning System), picture sharing by using Bluetooth pairing, data synchronising with laptop/desktop computers, document creation and modification, and entertainment (i.e., playing music). Indeed, the functionality and interconnectivity of mobile devices only tends to increase with time.

DOI: 10.4018/ijcwt.2011010105

While people enjoy the convenience provided by mobile devices, there are also threats which could make their life less comfortable, such as the loss or theft of the device, service fraud, information disclosure, mobile malware, Smishing (SMS [Short Message Service] phishing) and Vishing (Voice phishing). According to the metropolitan police website, there are around 10,000 mobile devices lost or stolen in London every month (Metropolitan Police Service, 2011). When a mobile device is lost or stolen, there is an initial cost of replacement; however, more damage could occur if the attacker accesses the mobile services and information. According to the Communications Fraud Control Association's (CFCA) Global Fraud Loss Survey 2009, service fraud is estimated to cost telecom service providers $72-$80 billion every year (CFCA, 2009). Also, a survey shows that 32% of all information disclosure incidents were related to lost or stolen mobile devices (Ponemon Institute, 2011). Moreover, the McAfee mobile and security report indicated that "Four in 10 organizations have had mobile devices lost or stolen and half of lost/stolen devices contain business critical data", such as customer data, corporate intellectual property and financial information (McAfee, 2011, p. 12).

Mobile malware can also harm the mobile phone in a variety of ways, such as: infecting files and damaging user data. Since first discovered in 2004, there are more than 106 malware families with 514 variants (Securelist, 2009). Furthermore, the number of new mobile malware being found in 2010 has increased considerably (by 46% compared with those occurring in 2009) (McAfee, 2010). Smishing and Vishing are new types of phishing attacks which are performed by utilising text messaging and telephone calls (FBI, 2010). If the phone owner is fooled, its personal information can be exposed and abused.

With the aim to counter mobile threats, a number of security mechanisms have been developed both on the mobile device and the service provider's network. The PIN (Personal Identification Number) based authentication method is the most widely deployed approach on mobile devices. Although widely used, many users do not employ the technique properly (i.e., never changing the PIN) (Clarke & Furnell, 2005; Kurkovsky & Syta, 2010). Mobile antivirus software and firewall applications are mainly deployed for detecting malware presence and blocking unwanted network traffic. Nonetheless, obtaining the latest virus signatures and updating rules for network traffic are not easy tasks; furthermore, their ability to detect user related activities is limited. As a mobile device has limited computing power, more sophisticated mechanisms, such as IDS (Intrusion Detection System), are primarily deployed on the service provider's network. These systems continuously monitor the mobile users' calling and migration activities to detect telephony service fraud. However, given the modern mobile device has the ability to access several networks simultaneously and accommodate a wide range of services, existing network-based security mechanisms are unable to provide comprehensive protection for the mobile handset. Therefore, a new security mechanism which can ensure a user's legitimacy (authentication function) in a continuous manner (IDS function) is needed. This paper focuses upon presenting the findings from a feasibility study into utilising a host-based behavioural profiling approach to identify mobile device misuse, and providing continued and transparent protection for mobile devices.

This paper begins by introducing various mobile device applications, mobile threats, and general security mechanisms and continues to describe the current state-of-the-art. A series of experimental studies on three aspects of user's applications usage (application-level, application-specific and overall) are presented in Section 3, with the following section describing the results. The paper then proceeds to discuss the results and conclude with highlighting the future direction of the research.

2. BEHAVIOUR-BASED MOBILE DEVICE SECURITY MECHANISMS

Research in mobile device security has been an established area for more than 10 years with a substantial amount of activity focused upon the areas of authentication, antivirus, firewalls, and IDS. Of particular interest however is the research that has been undertaken in behaviour-based mechanisms. This research falls primarily into two behaviour-based categories: network and host mechanisms.

Behaviour-Based *Network* Mobile Security Mechanisms

The research for studying mobile behaviour-based mechanisms started around 1995 mainly focusing upon the area of fraud detection. These mobile IDSs monitor user calling and migration behaviour over the service provider's network, and detect telephony service fraud (Gosset, 1998; Samfat & Molva, 1997; Boukerche & Nitare, 2002). One particularly successful approach is based upon developing a profile of users calling history over a period of time and comparing this historical profile against current usage, with deviations above a predefined threshold resulting in an alarm. Various supervised and unsupervised classifiers were successfully developed to deal with various attributes of the problem-space (known and unknown attack vectors) and the resulting systems were combined so that the strengths of each approach can be capitalised upon (Gosset, 1998).

Research has also focused on the use of geo-location information as a basis for detecting misuse. Based upon the hypothesis that people have a predictable travelling pattern, the migration based mobile IDS monitors a user's location activities to detect abnormal behaviour. The user's location information can be obtained either from the mobile cellular network (i.e., cell ID) or via a GPS link (i.e., longitude, latitude). By recording the users' location information over a time period, a mobility profile can be generated. When a mobile user carries their device from one location to another, the probability of the event will be calculated. If this surpasses a threshold, then the current event will be considered as an intrusion. A number of studies have been carried out by profiling user migration activities (Buschkes, Kesdogan, & Reichl, 1998; Hall, Barbeau, & Kranakis, 2005; Sun, Chen, Wang, Yu, & Leung, 2006).

By studying a user's calling or location activities, behaviour based IDSs can achieve a high detection rate and offer the ability to detect unforeseen attacks. In addition, as the classification and identification procedures are processed by the network service provider, it does not require any additional computational power from the mobile device. This has traditionally been critical for mobile devices, as they have limited processing power and storage when compared with traditional desktop computers.

Behaviour-Based *Host* Mobile Security Mechanisms

Existing host behaviour-based mobile security systems are mainly authentication-based systems being studied in the research field. These systems usually employ one or more characteristics of a user's behaviour to assess the legitimacy of the current user – techniques include and gait recognition, handwriting verification, keystroke analysis and voice verification.

Gait recognition is based upon the theory that people can be discriminated by how people walk when they carry their mobile device (Boyd & Little, 2005). When a user carries their mobile device in their trouser pocket, the user's gait information can be collected (Derawi, Nickel, Bours, & Busch, 2010). The user's gait data can then be compared with an existing template. If it matches, the user is considered legitimate; otherwise, they are an intruder. The experiment result shows that an EER (Equal Error Rate) of 20.1% can be achieved. It shows the possibility to deploy this method on a mobile handset. However, as the authentication process is heavily reliant on user's gait information, this could leave the mobile device unprotected when

gait information is not available – for example when the user sits in the office.

Handwriting verification: it is widely believed that each person has a unique handwriting style. Currently, a significant proportion of mobile devices have been equipped with a touch screen, enabling the handwriting verification technique to be deployed. A user's identity can be verified when they perform their signature (static) or while they write a message by using a stylus (dynamic). Clarke and Mekala (2007) proposed a dynamic approach to verify a user when certain words were written. With a 1% EER, their system performance was excellent. Despite their approach not being fully dynamic as the words were pre-chosen, their work demonstrated that it is possible to identify users based upon the way they write on a mobile device. Nonetheless, as the verification process is fully dependent upon user's handwriting activities, little protection can be provided if a user views a webpage or reads a document.

Keystroke analysis based authentication systems monitor users' keystroke patterns, typically monitoring the inter-keystroke latency and hold-time. The authentication can be performed in two modes: static (text dependent) and dynamic (text independent). In the static mode, users will be authenticated when a specific word or phrase has been entered. For instance, the system will authenticate the user when they enter a PIN to unlock their mobile devices. In the dynamic mode, a user's legitimacy will be checked based upon their typing speed and rhythm independent of what they type. For example, authentication will transparently occur while the user composes a text message. Previous work in this area includes Clarke and Furnell (2006), Buchoux and Clarke (2008), and Campisi, Maiorana, Bosco, and Neri (2009). With an average experimental EER of 13%, keystroke analysis based authentication systems can be deployed in practice to provide extra security for a mobile device. However, this method is only practical in scenarios with sufficient keystroke activity (i.e., activities such as reading a document or viewing a picture would be unlikely to generate sufficient data to successfully validate a users' identity).

Voice verification, also known as speaker recognition is based upon the way people speak. Traditionally, mobile devices were primarily used for making telephone calls, during which a user's voice sample can be captured for the purpose of voice verification. Woo, Park, and Hazen (2006) examined the possibility of using static voice verification for the mobile device by using an ASR-dependent speaker verification approach. Despite the comparison process being carried out by a standard computer, their work achieved a 7.8% EER proving that a user's identity can be verified by their voice, even in a noisy environment (i.e., in an office). Nevertheless, again, a user can only be authenticated during a conversation but not for other occasions.

Summary of Current Mobile Behaviour Security Mechanisms

The aforementioned literature suggests that existing behaviour-based network IDSs can detect calling service fraud attacks. However, in practice it can be seen that the mobile network operator can only monitor calling and migration behaviours, rather than examining every single mobile service. For the existing host-based behaviour authentication system, it could only provide periodically security when the user interacts with the device in the desired manner (e.g., when the keypad is touched or the device is carried in the back pocket). Therefore, none of the current research in mobile behaviour security mechanisms provides a comprehensive and continuous protection against device misuse. Hence, a mobile security mechanism which can offer continuous detection across a wider range of services and connections on the mobile device is needed.

Table 1. The MIT reality dataset

Activity	Number of Logs	Information Contains
General Applications	662,393	Application name, date, time of usage and cell ID
Voice Call	54,440	Date, time, number of calling, duration and cell ID
Text Message	5,607	Date, time, number of texting and cell ID

3. BEHAVIOUR PROFILING FOR TRANSPARENT AUTHENTICATION FOR MOBILE DEVICES

The previous section shows that the network-based behavioural security mechanisms can only monitor network-based services through the service provider's network. As current mobile devices have the ability to access multiple networks simultaneously, a host based approach must be taken into consideration when designing the new system. Furthermore, with the difficulty of obtaining and updating the signatures and the lack of the ability to detect unforeseen threats, a behaviour profiling technique would be prudent. As application usage represents an overview of how the user interacts with the device (Miettinen, Halonen, & Hatonen, 2006), and due to the lack of research regarding the discriminatory nature of application usage within a mobile device environment, an experiment was developed focused on three aspects: application-level, application-specific and multi-instance (or fused) applications interactions.

Experiment Procedure

The experiment employed a publicly available dataset provided by the MIT Reality Mining project (Eagle, Pentland, & Lazer, 2009). The dataset contains 106 participants' mobile phone activities from September 2004 to June 2005. By using preinstalled logging software, various mobile data attributes were collected from participants' using Nokia 6600 mobile phones. As shown in Table 1, the MIT Reality dataset contains a large and varied selection of information which covers two levels of application usage: application-level information (general applications) and application-specific information (voice call and text message).

Application-Level Analysis

By default, a number of common applications are preinstalled on the mobile device by the manufacture, such as: phonebook, clock and voice calling. With increased computing processing power and storage space and almost 15,000 new mobile applications becoming available on the market every month, mobile users have the freedom of installing any additional applications on the device (Distimo, 2010); this option completely changed the way that people utilise their mobile devices: from a dummy handset into a personalised computing gadget. From a high-level perspective the general use of applications can provide a basic level of information on how the mobile user utilises the device. Such basic information could be the name of the application, time, and location of usage. Given the hypothesis that mobile users utilise their mobile applications differently (i.e., two users utilise different applications in different time periods and at different locations), an experiment was devised to explore the possibility of utilising application-level information for discriminating mobile device users.

Application-Specific Analysis

The second experiment focused on utilising further information about the applications. Within many applications the user connects to data that could provide additional discriminatory information. For instance, when surfing the Internet, the Internet browser can capture all the

URLs an individual accesses. Unfortunately, due to limitations on the dataset (collected prior to data-based applications becoming prevalent), the range of application-specific analysis that could be undertaken were limited to telephony and text messaging.

The prior literature shows that calling behaviour has been studied several times in a network-based environment with results demonstrating the ability to discriminate mobile phone users. Within a mobile host environment, the availability of calling features does change slightly – for example, the IMSI (International Mobile Subscriber Identity) is not a useful feature in a host-based solution. Furthermore, although several studies suggested utilising a user's location information, it was never been treated as a calling feature. Therefore, it was interesting to identify the effectiveness of a new set of calling features, which included the user's location information.

Due to the enormous use of text messaging, with the UK alone sending more than 100 billion text messages in 2010 (Ofcom, 2010), the application is amongst the most widely used application on a mobile device. Despite the high volume of text message usage, little research has been undertaken to show how text messages may be used to detect abnormal usage in the mobile environment. Hence, it was also deemed important to discover the possibility and usefulness of employing text messaging to detect anomalous mobile user's behaviours.

Multi-Instance Analysis

The final experiment aimed at employing the multi-instance application usage to discriminate individual mobile users. In the experiment, all applications will be put in a chronological order – replaying what a user did with their mobile devices in the real time. For instance, a user switched off the clock alarm (application-level) at 6:05 AM, then visited a number of news websites (application-specific) at 6:20 AM, at 7:10 AM, he/she made several phone calls (application-specific), and started listening to the music (application-level) at 7:36 AM. Hence, the multi-instance applications can continuously present an image of what a user does on the whole, while either the application-level or application-specific applications could only partially provide information on user's activity. As a result, it is critical to explore the feasibility of utilising multi-instance applications for constantly monitoring every single activity to identify abnormal mobile usages.

For methodological reasons: to maximise the number of participants within a reasonable timeframe, the experiment employed 76 participants whose activities occurred during the period of 24/10/2004-20/11/2004. As not all participants started or finished the experiment at the same time, it was imperative to isolate a sub-section of the dataset that maximised the number of participants and available data. The methodology employed two types of profile techniques: static and dynamic. For the static profiling, each individual dataset was divided into two halves: the first half was used for building the profile, and the other half was utilised for testing. For the dynamic profiling, the profile contained 7/10/14 days of the user's most recent activities; the evaluation process was carried out on the same sub-dataset as for the static experiment in order to provide a meaningful comparison. Given the highly variable nature of the input data a smoothing function was applied. Rather than taking each individual result, the smoothing function permitted the system to make a decision after a number of results were present (similar to a winner-takes-all decision-based biometric fusion model). The basis for this approach was derived from the descriptive statistics produced when analysing the data and the large variances observed. A dynamic approach therefore seemed sensible to cope with the changing nature of the profile. Based on the premise that the historical profile can be used to predict the probability of a current event, the following formula illustrated in Equation 1 was devised. The equation also includes a weighting factor to allow for more discriminative features to have a greater contribution (W_i) within the resulting score than less discriminative features. Moreover, the equation

Table 2. Experimental results for application-level applications

		Number of Log Entries					
		1	2	3	4	5	6
Profile Technique	Static 14 days	21.1%	17.4%	16.3%	14.9%	14.2%	13.6%
	Dynamic 14 days	21.1%	17.3%	16.0%	14.5%	13.9%	13.5%
	Dynamic 10 days	22.1%	17.8%	16.2%	14.6%	14.4%	13.7%
	Dynamic 7 days	24.0%	19.4%	17.6%	15.9%	15.3%	14.4%

also provides a mechanism to ensure all outputs are bounded between 0 and 1 to assist in defining an appropriate threshold.

Equation 1: Alarm if:

$$1 - \frac{\sum_{i=1}^{N}\left(\frac{\text{Occurannce of Feature}_{ix}}{\sum_{x=1}^{M}\text{Occurannce of Feature}_{ix}} \times W_i\right)}{N} \geq \text{threshold}$$

Where:

i=The features of one chosen application (i.e., dialled number for telephony application) x=The value of Feature_i (i.e., office telephone number and home telephone number)

M=Total number of values for Feature_i

N=Total number of features

W_i=The weighting factor associated with Feature_i ($0 < W_i \leq 1$)

Threshold= A predefined value according to each individual user

4. EXPERIMENTAL RESULTS

Application-Level Profiling

For the general applications, the following features were extracted from the dataset: application name, date of initiation, and location of usage. As a total of 101 individual applications were used among the chosen 76 users during the chosen period, a final sub-dataset for application-level applications with 30,428 entry logs was formed. Among these 101 applications, the phonebook, call logs and camera were used by all participants. By using the proposed mathematical formula, a final set of EERs for users' application-level usage is presented in Table 2. The best EER is 13.5% and it was obtained by using the dynamic profile technique with 14 days of profiling data and a smoothing function with 6 log entries. In comparison, the worst performance was achieved by using the dynamic profile technique with 7 days of profiling data and the smoothing function with 1 log entry.

Selected results for the best configuration of the application-level applications experiment are shown in Table 3. The top 3 and bottom 3 users' EERs represent the best and worst performance respectively. Also, by using the same configuration, 84.2% of all users have an EER less than 20%.

Application-Specific Profiling

Telephony

For the telephone call application, a subset of 71 users from the 76 participants used the application during the aforementioned chosen period as other 5 users did not make any telephone calls. During the same period, 2,317 unique telephone numbers were dialled and the total number of calls made was 13,719. From iteration and optimisation, the following features were chosen for each log: the telephone number, date and location of call. By using the proposed mathematical formula with the selected features (all features were given the same weighting factor), a final set of experiment results is shown in Table 4. The best result is an EER of 5.4% and

Table 3. Selected users' performance for application-level applications with Dynamic 14 days and 6 log entries

User_ID	EER
71	0%
46	0%
12	0.5%
66	37.5%
2	39.3%
68	51.6%%

Table 4. Experimental results for telephone call application

		Number of Log Entries					
		1	2	3	4	5	6
Profile Technique	Static 14 days	9.6%	9.1%	7.9%	7.2%	4.3%	6.4%
	Dynamic 14 days	8.8%	8.1%	6.4%	6.4%	6.3%	5.4%
	Dynamic 10 days	9.6%	8.6%	8.1%	7.2%	6.9%	6.0%
	Dynamic 7 days	10.4%	8.8%	8.5%	7.3%	7.0%	6.2%

Table 5. Selected users' performance for telephone call application with Dynamic 14 days and 6 log entries

User_ID	Performance
23	0%
43	0%
61	0%
64	20.6%
50	23.1%
8	39.5%

it was achieved by using the dynamic profile technique with user's most recent 14 days of profiling data and a smoothing function with 6 log entries. While the worst EER if 10.4% and it was obtained by employing the dynamic profile with 7 days of profiling data and the smoothing function of 1 log entry.

A selection of results for the best set up of the telephone call application experiment is presented in Table 5. The best and worst performances for selected users are the top 3 and bottom 3 users accordingly. Also, 81.7% of users have an EER less than 10% with the same configuration.

Text Messaging

For the text messaging experiment, 22 users' text messaging activities were available from the 76 participants, while other 54 users did

Table 6. Experimental results for text messaging application

		Number of Log Entries		
		1	2	3
Profile Technique	Static 14 days	7.0%	4.3%	3.6%
	Dynamic 14 days	5.7%	2.6%	2.2%
	Dynamic 10 days	8.3%	4.1%	3.7%
	Dynamic 7 days	10.7%	5.7%	3.8%

Table 7. Selected users' performance for text messaging application with Dynamic 14 days and 3 log entries

User_ID	Performance
13	0%
14	0%
18	0.2%
4	5.3%
2	8.4%
17	13.1%

not send any text messages during the chosen period. The text messaging dataset contains 1,382 logs and 258 unique texting numbers. For each text log, the following features were extracted: receiver's telephone number, date and location of texting. Due to certain participants having limited numbers of text messaging logs; a maximum of 3 log entries were treated as one incident. By employing the proposed mathematical formula and all text message's features (all features were given the same weighting factor), the final result for user's text messaging application is shown in Table 6. The best result was an EER of 2.2% and it was acquired by utilising the dynamic profile method with 14 days of profiling data and a smoothing function with 3 log entries. Also, by increasing the smoothing function with 1 log entry to 2 log entries, the performance improves considerably across all profiling techniques.

Table 7 shows a group of users' performance for the best configuration of the text messaging application experiment. The top 3 and bottom 3 users' EERs represent the best and worst performance respectively. In addition, 95.5% of all users have an EER smaller than 10%.

Multi-Instance Profiling

For the multi-instance applications experiment, all 76 users' overall applications activities were utilised. For each user, its application-level applications and application-specific applications were joined together by using the time and day stamp in a chronological order. Also, features were selected according for the application-level and application-specific applications. In total, 30,428 application-level applications logs and 15,101 application-specific applications logs were employed for this set of experiment. By employing the proposed mathematical formula and various applications, the final results for users' multi-instance applications experiment are demonstrated in Table 8. By utilising the dynamic profiling technique with 10 days of

Table 8. Experimental results for multi-instance applications

		Number of Log Entries					
		1	2	3	4	5	6
Profile Technique	Static 14 days	16.9%	13.6%	12.7%	12%	10.9%	11%
	Dynamic 14 days	19%	15.2%	13.1%	12.4%	11.3%	10.5%
	Dynamic 10 days	17.1%	13.7%	12.3%	11.6%	10.6%	10%
	Dynamic 7 days	16.5%	13.5%	12.1%	11.6%	10.5%	10.1%

Table 9. Selected users' performance for multi-instance applications with Dynamic 10 days and 6 log entries

User_ID	Performance
46	0%
71	0%
63	0%
68	20.2%
69	25.4%
8	28.8%

profiling data and a smoothing function with 6 log entries, the best result of EER 10% was obtained. In comparison, the worst result of EER 19% was acquired by employing the dynamic profiling technique with 14 days of profiling data and the smoothing function with 1 log entry.

Table 9 illustrates a group of users' performance for the best configuration of the multi-instance applications experiment. The top 3 and bottom 3 users' EERs present the best and worst performance respectively. Also, 55.3% of all users have an EER smaller than 10% and 80.2% of all users have an EER lower than 15%.

5. DISCUSSION

The application name and location have proved valuable features that can provide sufficient discriminatory information to prove useful in authentication. However, whilst this might identify many misuse scenarios, it would not necessarily identify all cases of misuse – particular those where a colleague might temporarily misuse your device as the location information is likely to fall within the same profile as the authorised user. So care is required in interpreting these results. The application-specific and multi-instance approaches should also help to specifically identify this type of misuse.

In general, the dynamic profiling technique achieved a slightly better performance than the static profiling technique did. This is reasonable as a dynamic profile contains a user's most recent activities; hence it obtains a more accurate detection. With a longer training set period, the performance for application-level and application-specific application experiments is also improved. Hence, an increased number of days (i.e., 18/22 days) of user activities as the training set should be examined to find the optimum solution for these two sets of activities if a security system employs them individually. Nonetheless, literature suggests users do change their usage pattern over a long period of time. Farago (2009) suggests that users only keep 67% of the applications over a 30-day period. Moreover, storage and

processing issues should also be taken into consideration with larger training. In comparison, the multi-instance applications experiment obtained the best performance by using a training set period with 10 days of user's profiling data. As 10 days of user's profiling data might contain less information than a longer period of user's activities (i.e., 14 days), lower storage and processing power might be required when a security mechanism utilises multi-instance applications to verify a user. Nonetheless, as being based upon a period of days: some users have a lot of data while others potentially have very little, future work is required in order to determine what the optimum level of training profiling data is for the multi-instance activities. While a smoothing function treated more log entries as one incident, the performance also improved accordingly. The smoothing function reduces the impact any single event might have and seeks to take a more holistic approach to monitoring for misuse; this will provide a user-friendly environment as fewer rejections would occur and it would be more convenient when a user changes their usage behaviour. The disadvantage of this approach is that it takes more time for the system to make a decision; hence, an intruder could have more opportunities to abuse a system and a certain amount of abuse could be missed by the security control.

Limitations in the dataset are also likely to have created certain difficulties. As the dataset was collected in 2004, the number of mobile applications available for users to choose was limited; this resulted in a large similarity of application-level application usage between mobile users and hence increased difficulty for any classification methods. In contrast, in June 2011, there were around 1 million mobile applications available. As mobile users have more options, their application-level usage would arguably differ to a greater extent. Therefore, it would be easier to discriminate mobile users through their application-level usage.

As shown in Table 4, the performance of the telephony application experiment is very good – more than twice that of the application-level profiling. This reinforces the hypothesis that knowing both the application and what the user does with it, improves the chance of identifying individual users significantly. Moreover, mobile users had a far larger set of telephone contacts (the numbers they can dial) compared with the number of applications they had which also makes the classification process easier because there are more identifiable data points from which to discriminate. In comparison with other biometric authentication techniques (described in Section 2), the telephone experiment is within that category of performance.

As presented in Table 6, the results from the text messaging application experiment were even better than those achieved by the telephone call application, albeit with a smaller dataset. This may be caused by people only sending text messages to very close contacts. Although only 30% of the participants used the text messaging application in 2004, the situation has changed considerably: in the UK alone, the volume of text messaging traffic has increased by 290% since 2004 (Ofcom, 2010). This indicates that the text messaging based authentication method could serve a good proportion of the mobile users' population.

As demonstrated in Table 8, the experimental results for the multi-instance application are in between the results from the application-level and application-specific applications; this is within the expectation as the experiment utilised the combination of application-level and application-specific applications. Also, it is envisaged that the larger the proportion of application-specific applications users have, the better a system's performance. Hence, the process of differentiating whether an application belongs to the application-specific category and extracting its features accordingly is mission-critical for a behaviour profiling system.

From the results presented in this paper, it can be shown that both application-level, application-specific and multi-instance information can be used to authenticate mobile users. In addition, although it is more difficult to profile certain users, more than 80% of all users' performance was within the bounds of a behaviour-based biometric. The dynamic-based

profiling technique provides the opportunity to develop a more meaningful profile of user activities. This does however raise issues with regards to template ageing and ensuring the samples utilised in creating the template are all legitimate. Furthermore, in comparison with previous research, which used computationally complicated neural networks as the classification method (Li, Clarke, & Papadaki, 2009; Li, Clarke, Papadaki, & Dowland, 2010), this approach employed a light weight mathematical formula which saves a significant amount of processing power and storage space; this is essential for handheld mobile devices as they have limited processing power and storage space.

6. CONCLUSION

The experiment shows that with an EER of 13.5%, 5.4%, 2.2% and 10% for the general application, telephony, text messaging and multi-instance application usage respectively, these techniques are viable for a behaviour-based authentication mechanism within the mobile environment. The authentication process could be conducted in the background while mobile users utilise their applications; if several abnormal activities occurred within a fixed time frame, further security methods would be initiated according to the level of the incident.

Future work will focus upon designing an authentication architecture that could accommodate the aforementioned behaviour based authentication techniques. As the architecture works transparently in the background, little attention would be required from the mobile user and an intervention would only be needed when anomalous application usage occurs. Hence, such an architecture would provide a transparent and continuous protection for users. Furthermore, an operational system, which supports identity verification, will be developed for the purpose of evaluation.

REFERENCES

Boukerche, A., & Nitare, M. S. M. A. (2002). Behavior-Based Intrusion Detection in Mobile Phone Systems. *Journal of Parallel and Distributed Computing*, *62*(9), 1476–1490. doi:10.1006/jpdc.2002.1857

Boyd, J. E., & Little, J. J. (2005). Biometric gait recognition. In M. Tistarelli, J. Bigun, & E. Grosso (Eds.), *Proceedings of the Summer School on Biometrics* (LNCS 3161, pp. 19-42).

Buchoux, A., & Clarke, N. L. (2008). Deployment of Keystroke Analysis on a Smartphone. In C. Valli & A. Woodward (Eds.), *Proceedings of the 6th Australian Information Security & Management Conference* (pp. 40-47). Perth, WA, Australia: SECAU - Security Research Centre, Edith Cowan University.

Buschkes, R., Kesdogan, D., & Reichl, P. (1998). How to increase security in mobile networks by anomaly detection. In *Proceedings of the 14th Annual Computer Security Applications Conference* (pp. 3-12). Washington, DC: IEEE Computer Society.

Campisi, P., Maiorana, E., Bosco, M. L., & Neri, A. (2009). User authentication using keystroke dynamics for cellular phones. *IET Signal Processing*, *3*(4), 333–341. doi:10.1049/iet-spr.2008.0171

Clarke, N. L., & Furnell, S. M. (2005). Authentication of users on Mobile Telephones – A Survey of Attitudes and Practices. *Computers & Security*, *24*(7), 519–527. doi:10.1016/j.cose.2005.08.003

Clarke, N. L., & Furnell, S. M. (2006). Authenticating Mobile Phone Users Using Keystroke Analysis. *International Journal of Information Security*, *6*(1), 1–14. doi:10.1007/s10207-006-0006-6

Clarke, N. L., & Mekala, A. R. (2007). The application of signature recognition to transparent handwriting verification for mobile devices. *Information Management & Computer Security*, *15*(3), 214–225. doi:10.1108/09685220710759559

Communications Fraud Control Association (CFCA). (2009). *Communications Fraud Control Association (CFCA) announces results of worldwide telecom fraud survey.* Retrieved May 8, 2011, from http://www.cfca.org/pdf/survey/2009%20Global%20Fraud%20Loss%20Survey-Press%20Release.pdf

Derawi, M. O., Nickel, C., Bours, P., & Busch, C. (2010). Unobtrusive User-Authentication on Mobile Phones Using Biometric Gait Recognition. In I. Echizen (Ed.), *Proceedings of the 2010 6th International Conference on Intelligent Information Hiding and Multimedia Signal Processing* (pp. 306-311). Washington, DC: IEEE Computer Society.

Eagle, N., Pentland, A., & Lazer, D. (2009). Inferring Social Network Structure using Mobile Phone Data. [PNAS]. *Proceedings of the National Academy of Sciences of the United States of America*, *106*, 15274–15278. doi:10.1073/pnas.0900282106

Farago, P. (2009). *Mobile Apps: Models, Money and Loyalty.* Retrieved January 26, 2011, from http://blog.flurry.com/bid/26376/ Mobile-Apps-Models-Money-and-Loyalty Federal Bureau of Investigation (FBI). (2010). *Smishing and Vishing.* Retrieved December 12, 2010, from http://www.fbi.gov/news/stories/2010/november/cyber_112410/cyber_112410/

Gosset, P. (Ed.). (1998). *ASPeCT: Fraud Detection Concepts: Final Report* (Tech. Rep. No. AC095/VOD/W22/DS/P/18/1).

Gosteve, A., & Maslennikov, D. (2009). *Mobile Malware Evolution: An Overview, Part 3*. Retrieved March 30, 2011, from http://www.securelist.com/en/analysis?pubid=204792080

Hall, J., Barbeau, M., & Kranakis, E. (2005). Anomaly-based intrusion detection using mobility profiles of public transportation users. In *Proceedings of the IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob'2005)* (Vol. 2, pp. 17-24). Washington, DC: IEEE Computer Society.

Hoogsteder, V. (2010). *Our Presentation from Mobile World Congress 2010 – Mobile Application Stores State of Play.* Retrieved January 17, 2011, from http://blog.distimo.com/2010_02_our-presentation-from-mobile-world-congres-2010-mobile-application-stores-state-of-play/

Kurkovsky, S., & Syta, E. (2010). Digital natives and mobile phones: A survey of practices and attitudes about privacy and security. In K. Michael (Ed.), *Proceedings of the 2010 IEEE International Symposium on Technology and Society (ISTAS)* (pp. 441-449). Washington, DC: IEEE Computer Society.

Li, F., Clarke, N. L., & Papadaki, M. (2009). Intrusion DetectionSystem for Mobile Devices: Investigation on Calling Activity . In Dhillon, G. (Ed.), *Security, Assurance and Privacy: organizational challenges* (pp. 19.1–19.13). Washington, DC: Information Institute Publishing.

Li, F., Clarke, N. L., Papadaki, M., & Dowland, P. S. (2010). Behaviour Profiling on Mobile Devices. In G. Howells, K. Sirlantzis, A. Stoica, T. Huntsberger, & T. Arslan (Eds.), *Proceedings of the International Conference on Emerging Security Technologies* (pp. 77-82). Washington, DC: IEEE Computer Society.

McAfee. (2010). *McAfee Threats Report: Fourth Quarter 2010*. Retrieved March 30, 2011, from https://secure.mcafee.com/us/resources/reports/rp-quarterly-threat-q4-2010.pdf

McAfee. (2011). *Mobility and Security: Dazzling Opportunities, Profound Challenges*. Retrieved June 13, 2011, from http://www.mcafee.com/us/resources/reports/rp-cylab-mobile-security.pdf

Metropolitan Police Service. (2011). *Safeguarding your mobile phone.* Retrieved March 29, 2011, from http://www.met.police.uk/crimeprevention/phone.htm

Miettinen, M., Halonen, P., & Hatonen, K. (2006). Host-based intrusion detection for advanced mobile devices. In *Proceedings of the 20th International Conference on Advanced Information Networking and Applications (AINA'06)* (pp. 72-76). Washington, DC: IEEE Computer Society.

Ofcom. (2010). *Communications Market Report 2010*. Retrieved December 20, 2010, from http://stakeholders.ofcom.org.uk/binaries/research/cmr/753567/CMR_2010_FINAL.pdf

Ponemon Institute. (2011). *2010 Annual Study: U.K. Cost of a Data Breach*. Retrieved May 6, 2011, from http://www.symantec.com/content/en/us/about/media/pdfs/UK_Ponemon_CODB_2010_031611.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2011Mar_worldwide_costofdatabreach

Samfat, D., & Molva, R. (1997). IDAMN: an Intrusion Detection Architecture for Mobile Networks. *IEEE Journal on Selected Areas in Communications*, *15*(7), 1373–1380. doi:10.1109/49.622919

Sun, B., Chen, Z., Wang, R., Yu, F., & Leung, V. C. M. (2006). Towards adaptive anomaly detection in cellular mobile networks. In *Proceedings of the IEEE Consumer Communications and Networking Conference (CCNC 2006)* (Vol. 2, pp. 666-670). Washington, DC: IEEE Computer Society.

Woo, R., Park, A., & Hazen, T. (2006). The MIT Mobile Device Speaker Verification Corpus: Data collection and preliminary experiments. In *Proceedings of the 2006 Speaker and Language Recognition Workshop* (pp. 1-6). Washington, DC: IEEE Computer Society.

Behaviour Profiling for Transparent Authentication for Mobile Devices

Fudong Li[1], Nathan Clarke[1, 2], Maria Papadaki[1] and Paul Dowland[1]
[1]University of Plymouth, UK
[2]Edith Cowan University, Perth, Western Australia
info@cscan.org

Abstract: Since the first handheld cellular phone was introduced in 1970s, the mobile phone has changed significantly both in terms of popularity and functionality. With more than 4.6 billion subscribers around the world, it has become a ubiquitous device in our daily life. Apart from the traditional telephony and text messaging services, people are enjoying a much wider range of mobile services over a variety of network connections in the form of mobile applications. Although a number of security mechanisms such as authentication, antivirus, and firewall applications are available, it is still difficult to keep up with various mobile threats (i.e. service fraud, mobile malware and SMS phishing); hence, additional security measures should be taken into consideration. This paper proposes a novel behaviour-based profiling technique by using a mobile user's application usage to detect abnormal mobile activities. The experiment employed the MIT Reality dataset. For data processing purposes and also to maximise the number of participants, one month (24/10/2004-20/11/2004) of users' application usage with a total number of 44,529 log entries was extracted from the original dataset. It was further divided to form three subsets: two intra-application datasets compiled with telephone and message data; and an inter-application dataset containing the rest of the mobile applications. Based upon the experiment plan, a user's profile was built using either static and dynamic profiles and the best experimental results for the telephone, text message, and application-level applications were an EER (Equal Error Rate) of: 5.4%, 2.2% and 13.5% respectively. Whilst some users were difficult to classify, a significant proportion fell within the performance expectations of a behavioural biometric and therefore a behaviour profiling system on mobile devices is able to detect anomalies during the use of the mobile device. Incorporated within a wider authentication system, this biometric would enable transparent and continuous authentication of the user, thereby maximising user acceptance and security.

Keywords: mobile device, behaviour profiling, applications, transparent authentication

1. Introduction

The modern mobile handheld device is capable of providing many services through a wide range of applications over multiple networks as well as on the handheld itself, such as: voice calling through service provider's network, Internet surfing via Wi-Fi hotspots, video conferencing through a 3G connection, road navigating by GPS (Global Positioning System), picture sharing by using Bluetooth pairing, data synchronising with laptop/desktop computers, document creation and modification, and entertainment (i.e. playing music). Indeed, the functionality and interconnectivity of mobile devices only tends to increase with time.

While people enjoy the convenience provided by mobile devices, there are also threats which could make their life less comfortable, such as the loss or theft of the device, service fraud, SIM (Subscriber Identity Module) card cloning, mobile malware, information disclosure, DoS (Denial-of-Service) attacks, Smishing (SMS (Short Message Service) phishing) and Vishing (Voice phishing). Mobile malware could harm the mobile phone in a variety of ways, such as: infecting files and damaging user data. Since discovered in 2004, there are more than 106 malware families with 514 variants having been identified (Securelist 2010). Smishing and Vishing are new types of phishing attacks which are performed by utilising text messaging and telephone calls (FBI 2010). If the phone owner is fooled, its personal information can be exposed and abused.

With the aim to counter mobile threats, a number of security mechanisms have been developed both on the mobile device and the service provider's network. The PIN (Personal Identification Number) based authentication method is the most widely deployed approach on mobile devices. Although widely used, many users do not employ the technique properly (i.e. never changing the PIN) (Clarke and Furnell 2005; Kurkovsky and Syta 2010). Mobile antivirus software and firewall applications are mainly deployed for detecting malware presence and blocking unwanted network traffic. Nonetheless, obtaining the latest virus signatures and updating rules for network traffic are not easy tasks; furthermore, their ability to detect user related activities is limited. As a mobile device has limited computing power, more sophisticated mechanisms, such as IDS (Intrusion Detection System), are primarily deployed on the service provider's network. These systems monitor the mobile users' calling and migration activities to detect telephony service fraud. However, given the modern mobile device has the ability to access

several networks simultaneously and accommodate a wide range of services, existing network-based security mechanisms are unable to provide comprehensive protection for the mobile handset. This paper focuses upon presenting the findings from a feasibility study into utilising a host-based behavioural profiling approach to identify mobile device misuse, and providing continued and transparent protection for mobile devices.

This paper begins by introducing various mobile device applications, mobile threats, and general security mechanisms and continues to describe the current state-of-the-art. A series of experimental studies on two aspects of user's applications usage (application-level and application-specific) are presented in Section 3, with the following section describing the results. The paper then proceeds to discuss the results and conclude with highlighting the future direction of the research.

2. Behaviour-based mobile device security mechanisms

Research in mobile device security has been an established area for more than 10 years with a substantial amount of activity focused upon the areas of authentication, antivirus, firewalls, and IDS. Of particular interest however is the research that has been undertaken in behaviour-based mechanisms. This research falls primarily into two categories: behaviour-based network and behaviour-based host mechanisms.

2.1 Behaviour-based *network* mobile security mechanisms

The research for studying mobile behaviour-based mechanisms started around 1995 mainly focusing upon the area of IDS. These mobile IDSs monitor user calling and migration behaviour over the service provider's network, and detect telephony service fraud (Gosset 1998; Samfat and Molva 1997; Boukerche and Nitare 2002). One particularly successful approach is based upon developing a profile of users calling history over a period of time and comparing this historical profile against current usage, with deviations above a predefined threshold resulting in an alarm. Various supervised and unsupervised classifiers were successfully developed to deal with various attributes of the problem-space (known and unknown attack vectors) and the resulting systems were combined so that the strengths of each approach can be capitalised upon (Gosset 1998).

Research has also focused on the use of geo-location information as a basis for detecting misuse. Based upon the hypothesis that people have a predictable travelling pattern, the migration based mobile IDS monitors a user's location activities to detect abnormal behaviour. The user's location information can be obtained either from the mobile cellular network (i.e. cell ID) or via a GPS link (i.e. longitude, latitude). By recording the users' location information over a time period, a mobility profile can be generated. When a mobile user carries their device from one location to another, the probability of the event will be calculated. If this surpasses a threshold, then the current event will be considered as an intrusion. A number of studies have been carried out by profiling user migration activities, such as: Buschkes *et al* 1998, Hall *et al* 2005, and Sun *et al* 2006.

By studying a user's calling or location activities, behaviour based IDSs can achieve a high detection rate and offer the ability to detect unforeseen attacks. In addition, as the classification and identification procedures are processed by the network service provider, it does not require any additional computational power from the mobile device. This has traditionally been critical for mobile devices, as they have limited processing power and space comparing with traditional desktop computers. Nonetheless, if these behaviour-based systems work together to monitor the mobile user's action (i.e. calling a friend) while knowing where the action is taken (i.e. at home), an overall system performance could arguably be increased.

2.2 Behaviour-based *host* mobile security mechanisms

Existing host behaviour-based mobile security systems are mainly authentication-based systems. These systems usually employ one or more characteristics of a user's behaviour to assess the legitimacy of the current user – techniques include keystroke analysis and gait recognition.

Keystroke analysis based authentication systems monitor users' keystroke patterns, typically monitoring the inter-keystroke latency and hold-time. The authentication can be performed in two modes: static (text dependent) and dynamic (text independent). In the static mode, users will be authenticated when a specific word or phrase has been entered. For instance, the system will authenticate the user when they enter a PIN to unlock their mobile devices. In the dynamic mode, a user's legitimacy will be checked

based upon their typing speed and rhythm independent of what they type. For example, authentication will transparently occur while the user composes a text message. Previous work in this area include Clarke and Furnell (2006), Buchoux and Clarke (2008), and Campisi *et al.* (2009). With an average experimental EER of 13%, keystroke analysis based authentication systems can be deployed in practice to provide extra security for a mobile device. However, this method is only practical in scenarios with sufficient keystroke activity (i.e. activities such as reading a document or viewing a picture would be unlikely to generate sufficient data to successfully validate a users' identity).

Gait recognition is based upon the theory that people can be discriminated by how people walk when they carry their mobile device (Boyd and Little, 2005). When a user carries their mobile device in their trouser pocket, the user's gait information can be collected (Derawi *et al* 2010). The user's gait data can then be compared with an existing template. If it matches, the user is considered legitimate; otherwise, they are an intruder. The experiment result shows that an EER of 20.1% can be achieved. It shows the possibility to deploy this method on a mobile handset. However, as the authentication process is heavily reliant on user's gait information, this could leave the mobile device unprotected when gait information is not available – for example when the user sits in the office.

2.3 Summary of current mobile behaviour security mechanisms

The aforementioned literature suggests that existing behaviour-based network IDSs can detect calling service fraud attacks. However, in practice it can be seen that the mobile network operator can only monitor calling and migration behaviours, rather than examining every single mobile service. For the existing host-based behaviour authentication system, it could only provide periodically security when the user interacts with the device in the desired manner (e.g. when the keypad is touched or the device is carried in the back pocket). Therefore, none of the current research in mobile behaviour security mechanisms provides a comprehensive and continuous protection against device misuse. Hence, a mobile security mechanism which can offer detection across a wider range of services and connections on the mobile device is needed.

3. Behaviour profiling for transparent authentication for mobile devices

The previous section shows that the network-based behavioural security mechanisms can only monitor network-based services through the service provider's network. As current mobile devices have the ability to access multiple networks simultaneously, a host based approach must be taken into consideration when designing the new system. With the difficulty of obtaining and updating the signatures and the lack of the ability to detect unforeseen threats, a behaviour profiling technique should be taken. As application usage represents an overview of how the user interacts with the device (Miettinen *et al* 2006), and due to the lack of research regarding the discriminatory nature of application usage within a mobile device environment, an experiment was developed focussing upon two aspects: application-level and application-specific user interactions.

3.1 Experiment procedure

The experiment employed a publicly available dataset provided by the MIT Reality Mining project (Eagle *et al* 2009). The dataset contains 106 participants' mobile phone activities from September 2004 to June 2005. By using preinstalled logging software, various mobile data attributes were collected from participants' using Nokia 6600 mobile phones. As shown in Table 1, the MIT Reality dataset contains a large and varied selection of information which covers two levels of application usage: application-level information (general applications) and application-specific information (voice call and Text message).

Table 1: The MIT Reality dataset

Activity	Number of logs	Information contains
General applications	662,393	Application name, date, time of usage and cell ID
Voice call	54,440	Date, time, number of calling, duration and cell ID
Text message	5,607	Date, time, number of texting and cell ID

3.1.1 Application-level analysis

By default, a number of common applications are preinstalled on the mobile device by the manufacture, such as: phonebook, clock and voice calling. With increased computing processing power and storage space and almost 15,000 new mobile applications becoming available on the market every month, mobile

users have the freedom of installing any additional applications on the device (Distimo 2010). From a high-level perspective the general use of applications can provide a basic level of information on how the mobile user utilises the device. Such basic information could be the name of the application, time, and location of usage. Given the hypothesis that mobile users utilise their mobile applications differently (i.e. two users utilise different applications in different time periods and at different locations), an experiment was devised to explore the possibility of utilising application-level information for discriminating mobile device users.

3.1.2 Application-specific analysis

The second experiment focussed upon utilising further information about the applications. Within many applications the user connects to data that could provide additional discriminatory information. For instance, when surfing the Internet, the Internet browser can capture all the URLs an individual accesses. Unfortunately, due to limitations on the dataset (collected prior to data-based applications becoming prevalent), the range of application-specific analysis that could be undertaken were limited to telephony and text messaging.

The prior literature shows that calling behaviour has been studied several times in a network-based environment with results demonstrating the ability to discriminate mobile phone users. Within a mobile host environment, the availability of calling features does change slightly – for example, the IMSI (International Mobile Subscriber Identity) is not a useful feature in a host-based solution. Furthermore, although several studies suggested utilising a user's location information, it was never been treated as a calling feature. Therefore, it was interesting to identify the effectiveness of a new set of calling features, which included the user's location information.

Due to the enormous use of text messaging, with the UK alone sending more than 100 billion text messages in 2010 (Ofcom 2010), the application is amongst the most widely used application on a mobile device. Despite the high volume of text message usage, little research has been undertaken to show how text messages may be used to detect abnormal usage in the mobile environment. Hence, it was also deemed important to discover the possibility and usefulness of employing text messaging to detect anomalous mobile user's behaviours.

For methodological reasons: to maximise the number of participants within a reasonable timeframe, the experiment employed 76 participants whose activities occurred during the period of 24/10/2004-20/11/2004. As not all participants started or finished the experiment at the same time, it was imperative to isolate a sub-section of the dataset that maximised the number of participants and available data. The methodology employed two types of profile techniques: static and dynamic. For the static profiling, each individual dataset was divided into two halves: the first half was used for building the profile, and the other half was utilised for testing. For the dynamic profiling, the profile contained 7/10/14 days of the user's most recent activities; the evaluation process was carried out on the same sub-dataset as for the static experiment in order to provide a meaningful comparison. Given the highly variable nature of the input data a smoothing function was applied. Rather than taking each individual result, the smoothing function permitted the system to make a decision after a number of results were present (similar to a winner-takes-all decision-based biometric fusion model). The basis for this approach was derived from the descriptive statistics produced when analysing the data and the large variances observed. A dynamic approach therefore seemed sensible to cope with the changing nature of the profile. Based on the premise that the historical profile can be used to predict the probability of a current event, the following formula illustrated in Equation 1 was devised. The equation also includes a weighting factor to allow for more discriminative features to have a greater contribution (W_i) within the resulting score than less discriminative features. Moreover, the equation also provides a mechanism to ensure all outputs are bounded between 0 and 1 to assist in defining an appropriate threshold.

Equation 1: Alarm if: $$1-\frac{\sum_{i=1}^{N}\left(\frac{\text{Occurannce of Feature}_{in}}{\sum_{x=1}^{M}\text{Occurannce of Feature}_{in}}\times W_i\right)}{N}$$ ≥threshold

Where:

i=The features of one chosen application (i.e. dialled number for telephony application)

x=The value of Feature$_i$ (i.e. office telephone number and home telephone number)

M=Total number of values for Feature$_i$

N=Total number of features

W_i=The weighting factor associated with Feature$_i$ ($0 < W_i \leq 1$)

Threshold= A predefined value according to each individual user

4. Experimental results

4.1 Application-level profiling

For the general applications, the following features were extracted from the dataset: application name, date of initiation, and location of usage. As a total of 101 individual applications were used among the chosen 76 users during the chosen period, a final sub-dataset for application-level applications with 30,428 entry logs was formed. Among these 101 applications, the phonebook, call logs and camera were used by all participants. By using the proposed mathematical equation, a final set of EER's (Equal Error Rate) for users' application-level usage is presented in Table 2. The best EER is 13.5% and it was obtained by using the dynamic profile technique with 14 days of user activity with 6 log entries. In comparison, the worst performance was achieved by using the dynamic profile technique with 7 days of user activities with 1 log entry.

Table 2: Experimental results for application-level applications

		Number of log entries					
		1	2	3	4	5	6
Profile technique	Static 14 days	21.1%	17.4%	16.3%	14.9%	14.2%	13.6%
	Dynamic 14 days	21.1%	17.3%	16.0%	14.5%	13.9%	13.5%
	Dynamic 10 days	22.1%	17.8%	16.2%	14.6%	14.4%	13.7%
	Dynamic 7 days	24.0%	19.4%	17.6%	15.9%	15.3%	14.4%

Selected experimental results for the best configuration of application-level usage are shown in Table 3. The top 3 and bottom 3 users' EERs represent the best and worst performance respectively. Further analyses of the results show that 84% of all users have an EER less than 20%.

Table 3: Selected users' performance for application-level applications with dynamic 14 days and 6 log entries

User_ID	EER
71	0%
46	0%
12	0.5%
66	37.5%
2	39.3%
68	51.6%%

4.2 Application-specific profiling

4.2.1 Telephony

For the telephone call application, a subset of 71 users from the 76 participants used the application during the aforementioned chosen period. During the same period, 2,317 unique telephone numbers were dialled and the total number of calls made was 13,719. From iteration and optimisation, the following features were chosen for each log: the telephone number, date and location of call. By using the aforementioned mathematical formula with the selected features (all features were given the same weighting factor), a final set of experiment results is shown in Table 4. The best result is an EER of 5.4% and it was achieved by using the dynamic profile technique with user's most recent 14 days activity and 6 log entries.

Table 4: Experimental results for telephone call application

		Number of log entries					
		1	2	3	4	5	6
Profile technique	Static 14 days	9.6%	9.1%	7.9%	7.2%	4.3%	6.4%
	Dynamic 14 days	8.8%	8.1%	6.4%	6.4%	6.3%	5.4%
	Dynamic 10 days	9.6%	8.6%	8.1%	7.2%	6.9%	6.0%
	Dynamic 7 days	10.4%	8.8%	8.5%	7.3%	7.0%	6.2%

A selection of experimental results for the best set up of the telephone call application is presented in Table 5. The best and worst performances for selected users are the top 3 and bottom 3 users accordingly. Furthermore, 81.7% of users have an EER less than 10%.

Table 5: Selected users' performance for telephone call application with Dynamic 14 days and 6 log entries

User_ID	Performance
23	0%
43	0%
61	0%
64	20.6%
50	23.1%
8	39.5%

4.2.2 Text messaging

For the text messaging experiment, 22 users' text messaging activities were available from the 76 participants, during the chosen period. The text messaging dataset contains 1,382 logs and 258 unique texting numbers. For each text log, the following features were extracted: receiver's telephone number, date and location of texting. Due to certain participants having limited numbers of text messaging logs; a maximum of 3 log entries were treated as one incident. By employing the aforementioned mathematical formula and all text message's features (all features were given the same weighting factor), the final result for user's text messaging application is shown in Table 6. The best result was an EER of 2.2% and it was acquired by utilising the dynamic profile method with 14 days of user's activities and 3 log entries. Also, the performance improves considerably from 1 log entry to 2 log entries across all profiling techniques.

Table 6: Experimental results for text messaging application

		Number of log entries		
		1	2	3
Profile technique	Static 14 days	7.0%	4.3%	3.6%
	Dynamic 14 days	5.7%	2.6%	2.2%
	Dynamic 10 days	8.3%	4.1%	3.7%
	Dynamic 7 days	10.7%	5.7%	3.8%

Table 7 shows a group of users' performance for the best configuration of the text messaging application. The top 3 and bottom 3 users' EERs represent the best and worst performance respectively. In addition, 95.5% of all users have an EER smaller than 10%.

Table 7: Selected users' performance for text messaging application with Dynamic 14 days and 6 log entries

User_ID	Performance
13	0%
14	0%
18	0.2%
4	5.3%
2	8.4%
17	13.1%

5. Discussion

The application name and location have proved valuable features that can provide sufficient discriminatory information to prove useful in authentication. However, whilst this might identify many misuse scenarios, it would not necessary identify all cases of misuse – particular those where a colleague might temporarily misuse your device as the location information is likely to fall within the same profile as the authorised user. So care is required in interrupting these results. The intra-application approach should also help to specifically identify this type of misuse.

In general, dynamic profiling achieved a slightly better performance than the static profiling did. This is reasonable as a dynamic profile contains a user's most recent activities; hence it obtains a more accurate detection. Furthermore, with a longer training set period, the performance is also improved. Hence, an increased number of days (i.e. 18/22 days) of user activities as the training set should be examined to find the optimum solution. Nonetheless, literature suggests users do change their usage pattern over a long period of. A study by Flurry (2009) states that users only keep 67% of the applications over a 30 days period. Moreover, storage and processing issues should also be taken into consideration with larger training. While a smoothing function treated more log entries as one incident, the performance also improved accordingly. The smoothing function reduces the impact any single event might have and seeks to take a more holistic approach to monitoring for misuse. The disadvantage of this approach is that it takes a longer time for the system to make a decision; hence, an intruder could have more opportunities to abuse a system and a certain amount of abuse could be missed by the security control.

Limitations in the dataset are also likely to have created certain difficulties. As the dataset was collected in 2004, the number of mobile applications available for users to choose was limited; this resulted in a large similarity of application-level application usage between mobile users and difficulty for any classification methods. In contrast, in the early part of 2010, there were around 200,000 mobile applications available (Distimo 2010). As mobile users have more options, their application-level usage would arguably differ larger. Therefore, it would be easier to discriminate mobile users through their application-level usage.

As shown by Table 4, the performance of the telephony application is very good – more than twice that of the application-level profiling. This reinforces the hypothesis that knowing both the application and what the user does with it, improves the chance of identifying individual users significantly. Moreover, mobile users had a far larger set of telephone contacts (the numbers they can dial) compared with the number of applications they had also makes the classification process easier because there are more identifiable data points from which to discriminate. In comparison with other biometric authentication techniques such as keystroke analysis, which has an average EER of 8%, the telephone experiment is within that category of performance (Clarke and Furnell 2006).

As presented in Table 6, the results from the text messaging application were even better than those achieved by the telephone call application, albeit with a smaller dataset. This may be caused by people only sending text messages to very close contacts. Although only 30% of the participants used the text messaging application in 2004, the situation has changed considerably: for UK alone, the volume of text messaging traffic has increased by 290% since 2004 (Ofcom 2010). This indicates that the text messaging based authentication method could serve a good proportion of the mobile users' population.

From the results presented in this paper, it can be shown that both application-level and application-specific information can be used to authenticate mobile users. In addition, although it is more difficult to profile certain users, more than 81% of all users' performance was within the bounds of a behaviour-based biometric. Dynamic-based profiling technique provides the opportunity to develop a more meaningful profile of user activities. This does however raise issues with regards to template aging and ensuring the samples utilised in creating the template are all legitimate that will need to be addressed. Furthermore, in comparison with previous research, which used computationally complicated neural networks as the classification method (Li *et al* 2009; Li *et al* 2010), this approach employed a light weight mathematical formula which saves a significant amount of processing power and storage space; this is essential for handheld mobile devices as they have limited processing power and storage space.

6. Conclusions

The experiment shows that with an EER of 5.4%, 2.2% and 13.5% for the telephony, text messaging and general application usage respectively, and these techniques are viable for a behaviour-based

authentication mechanism within the mobile environment. The authentication process could be carried in the background while mobile users utilise their applications; if several abnormal activities occurred within a fixed time frame, further security methods would be initiated according to the level of the incident.

Future work will focus upon designing an authentication architecture that could accommodate the aforementioned behaviour based authentication techniques. As the architecture works behind the scene, little attention would be required from the mobile user and an intervention would only be needed when anomalous application usage occurs. Hence, such an architecture would provide a transparent and continuous protection for users. Furthermore, an operational system, which supports identity verification, will be developed for the purpose of evaluation.

References

Boukerche, A. and Nitare, M.S.M.A. (2002) “Behavior-Based Intrusion Detection in Mobile Phone Systems”, Journal of Parallel and Distributed Computing, vol. 62, Issue 9, pp. 1476-1490, Academic Press, Inc. Orlando, FL, USA

Boyd, J.E., and Little, J.J. (2005) “Biometric gait recognition”, Advanced Studies in Biometrics: Summer School on Biometrics, pp19-42, 2005, LCNS

Buchoux A, Clarke NL (2008) Deployment of Keystroke Analysis on a Smartphone, Proceedings of the 6th Australian Information Security & Management Conference, 1-3 December, Perth, Australia

Buschkes, R., Kesdogan, D. and Reichl, P. (1998) “How to increase security in mobile networks by anomaly detection”, Proceedings of the 14th Annual Computer Security Applications Conference, pp. 3-12. IEEE Computer Society, Washington, DC, USA

Campisi, P., Maiorana, E., Bosco, M.L., Neri, A. (2009) "User authentication using keystroke dynamics for cellular phones", IET Signal Processing, Vol.3 No.4 pp333-41

Clarke, N.L. and Furnell, S.M. (2005) “Authentication of users on Mobile Telephones – A Survey of Attitudes and Practices”, Computer & Security, 24(7), pp.519-527

Clarke, N.L. and Furnell, S.M. (2006) “Authenticating Mobile Phone Users Using Keystroke Analysis”, International Journal of Information Security, ISSN:1615-5262, pp.1-14

Derawi, M.O., Nickel, C., Bours, P., and Busch, C. (2010) "Unobtrusive User-Authentication on Mobile Phones Using Biometric Gait Recognition," Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2010

Distimo, (2010) “Our Presentation From Mobile World Congres 2010 – Mobile Application Stores State Of Play”, [online], http://blog.distimo.com/2010_02_our-presentation-from-mobile-world-congres-2010-mobile-application-stores-state-of-play/, date accessed: 17 January 2011Eagle, N., Pentland, A. and Lazer, D. (2009) “Inferring Social Network Structure using Mobile Phone Data”, Proceedings of the National Academy of Sciences (PNAS), vol 106, pp.15274-15278.

FBI (2010) “Smishing and Vishing”, [online], http://www.fbi.gov/news/stories/2010/november/cyber_112410/cyber_112410, date of access: 02/12/2010

Flurry (2009) “Mobile Apps: Models, Money and Loyalty”, [online], http://blog.flurry.com/bid/26376/ Mobile-Apps-Models-Money-and-Loyalty, date accessed: 26 January 2011

Gosset, P. (1998) “ASPeCT: Fraud Detection Concepts: Final Report”, Doc Ref. AC095/VOD/W22/DS/P/18/1

Hall, J., Barbeau, M. and Kranakis, E. (2005) “Anomaly-based intrusion detection using mobility profiles of public transportation users”, the Proceeding of IEEE International Conference on Wireless And Mobile Computing, Networking And Communications, 2005 (WiMob'2005), vol. 2, pp.17-24.

Kurkovsky, S. and Syta, E. (2010) “Digital natives and mobile phones: A survey of practices and attitudes about privacy and security”, In Proceedings of the 2010 IEEE International Symposium on Technology and Society (ISTAS), pp. 441-449

Li, F., Clarke, N.L. and Papadaki, M. (2009) “Intrusion DetectionSystem for Mobile Devices: Investigation on Calling Activity”, Proceedings of the 8th Security Conference, April, Las Vegas, USA

Li, F., Clarke, N.L., Papadaki, M. and Dowland, P.S. (2010) “Behaviour Profiling on Mobile Devices”, International Conference on Emerging Security Technologies, 6-8 September, Canterbury, UK, pp.77-82

Miettinen, M., Halonen, P., and Hatonen, K. (2006) “Host-based intrusion detection for advanced mobile devices”, Proceedings of the 20th International Conference on Advanced Information Networking and Applications (AINA’ 06), pp 72-76

Ofcom, (2010) “Communications Market Report, 2010”, [online], http://stakeholders.ofcom.org.uk/binaries/research/cmr/753567/CMR_2010_FINAL.pdf, date accessed: 20 December 2010

Samfat, D. and Molva, R. (1997) “IDAMN: an Intrusion Detection Architecture for Mobile Networks”, IEEE Journal on Selected Areas in Communications, vol. 15, pp.1373-1380.

Securelist, (2010) “Mobile Malware Evolution: An Overview, Part 3”, [online], http://www.securelist.com/en/analysis?pubid=204792080, date of access: 03/12/2010

Sun, B., Chen, Z., Wang, R., Yu, F. and Leung, V.C.M. (2006) “Towards adaptive anomaly detection in cellular mobile networks”, the IEEE Consumer Communications and Networking Conference, 2006 (CCNC 2006), Vol. 2, pp. 666-670, IEEE

Behaviour Profiling on Mobile Devices

Fudong Li[1], Nathan Clarke[1,2], Maria Papadaki[1], Paul Dowland[1]

[1] *Centre for Security, Communications and Network Research (CSCAN), School of Computing & Mathematics, University of Plymouth, Plymouth, PL4 8AA, United Kingdom*
info@cscan.org
[2] *School of Computer and Information Science, Edith Cowan University, Perth, Western Australia*

Abstract

Over the last decade, the mobile device has become a ubiquitous tool within everyday life. Unfortunately, whilst the popularity of mobile devices has increased, a corresponding increase can also be identified in the threats being targeted towards these devices. Security countermeasures such as AV and firewalls are being deployed; however, the increasing sophistication of the attacks requires additional measures to be taken. This paper proposes a novel behaviour-based profiling technique that is able to build upon the weaknesses of current systems by developing a comprehensive multi-level approach to profiling. In support of this model, a series of experiments have been designed to look at profiling calling, device usage and Bluetooth network scanning. Using neural networks, experimental results for the aforementioned activities' are able to achieve an EER (Equal Error Rate) of: 13.5%, 35.1% and 35.7%.

1. Introduction

Over the last decade, the mobile device has changed significantly; becoming a multimedia and multi-functional device. The mobile telephone alone, a subset of the mobile devices, has over 4.1 billion subscribers around the world. The modern mobile device is capable of providing a wide range of services over several network connections on a continual basis. As a result, many people rely upon these services and information to complete their business and personal tasks. Such tasks can include accessing email via a wireless network, online shopping through a 3G network, sharing pictures over a Bluetooth connection, and reading documents. The nature of many of these activities is likely to be either personally or corporately sensitive.

While people enjoy the convenience and pleasure the mobile device provides, it can also bring several security concerns, such as service fraud, lost or stolen handsets, SIM (Subscriber Identity Module) card cloning [1], malware, information disclosure, and Denial of Service (DoS) [2]. For the malware alone, although it was discovered a few years ago, the number of incidents is growing significantly every year. For instance, Kaspersky have already identified a total number of 106 mobile malware families with 514 modifications since 2004 [3].

To counter these security threats, various mobile security solutions have been proposed and developed in the area of authentication, firewalls and antivirus. However, given the increasing sophistication of the threats, additional countermeasures present in the desktop environment are being considered for use on a mobile device. Intrusion Detection Systems (IDSs) are one such technology. Unfortunately, the current nature of IDSs deployed within the desktop environment is significantly different to the mobile environment, with differing stakeholders, requirements and capabilities. In addition, research to date in the area of mobile IDS has been limited to identifying specific threats rather than taking a comprehensive approach [4]. This paper focuses upon presenting the findings from a feasibility study into utilising behavioural profiling to successfully identify mobile device misuse.

This paper begins by introducing the threats associated with a mobile device, and general security controls. Section 2 identifies the key research completed to date. Section 3, presents the methodology for a series of experimental studies on three aspects of mobile user's behaviours: telephony, device usage, and Bluetooth scanning. The results from the experiments are presented along with the discussion in section 4. The paper then proceeds to propose a Host-based Multi-Level Behaviour Profiling Mobile IDS framework. The paper concludes with highlighting the future work.

2. Mobile Intrusion Detection System

The IDS is an established research area for more than 20 years. There is extensive research on computer-based IDSs, but limited emphasis has been given so far on mobile IDSs. So, the focus of this section is to review existing research on mobile IDS: namely behaviour-based and signature-based IDSs.

978-0-7695-4175-4/10 $26.00 © 2010 IEEE
DOI 10.1109/EST.2010.26

2.1. Behaviour Based Mobile IDS

The research for mobile IDS started around 1995 with preliminary focus upon detecting telephony service fraud. By monitoring users' calling behaviour and migration activity, the aforementioned attack can be detected.

The telephony based mobile IDS monitors user's calling features (e.g. start time of call, duration of call, dialled telephone number and national or international call). By using the combination of these features, a historical profile is acquired. Any deviation between the current calling session and the historical profile that exceeds a threshold, is identified as an intrusion. Several studies were proposed by using this procedure, such as the European ASPECT (Advanced Security for Personal Communication Technologies) project [5], [6], and [7].

Migration based mobile IDS monitors the mobile user's migration activities through mobile cell networks. By profiling a mobile user's migration mobility or migration itinerary activities, telephony service frauds could be detected. A number of studies have been carried out by using users' migration activity: [8-9] employed user's mobility, and [10] used user's migration itinerary.

In generally, behaviour based mobile IDS has an average high detection rate; also, as the detection process is carried out by the network operator, there is no overhead for the mobile device. On the other hand, as the mobile device has changed significantly, the network operator could not monitor all the behaviour any more such as Internet surfing over WiFi networks.

2.2. Signature Based Mobile IDS

It is widely recognised that the battery plays a key role in a mobile device. Attacking the battery is a major threat for the mobile device's availability; as the battery runs out, the device becomes unusable. In order to counter battery consumption as a result of security threats, such as malware and DoS, several studies on signature based mobile IDS have been conducted: such as, Power Secure Architecture [11], and Gibraltar [12]. They work in a similar fashion: each mobile application consumes unique power and so does the malware. As a result, by analysing battery activities, attacking signatures can be obtained. By comparing the current battery status with attacking signatures, any matches will be identified as an intrusion.

The advantage for the signature based mobile IDS is it has a low false alarm rate and meaningful descriptions for the intrusion. However, obtaining mobile malware's signatures can be a difficult task; furthermore, it can not provide detection for service related attacks such as abusing the telephony service or data modification on the mobile device.

2.3. Summary Of Current Mobile IDS

From the aforementioned literature, it suggests that the behaviour based mobile IDS is able to detect telephony service fraud attacks and the signature based mobile IDS can identify possible malware and DoS attacks. However, in practice it can be seen that the calling and migration behaviours were monitored by a single network provider, rather than being host-based, and the signature based mobile IDSs have limited signatures in the database and thus cannot provide much detection for user related activities. In addition, as increased functionality, usability and compatibility, users are now experiencing a far larger set of mobile activities illustrated in the last column of Table 1. Therefore none of the current research in mobile IDS truly provides a compressive protection against device misuse independent of service or application being used. As a result, a mobile IDS which can offer the detection for a wider range of services and connections on the mobile device is certainly needed.

Table 1. Taxonomy of mobile usage

Category	Behaviours	Examples
Application level	Telephony	Call a friend
	Text	Send greeting through SMS
	MMS	Send picture through MMS
	File access	Write and save a document
	Data	Create a copy of work data
	Web	Read news from the internet
Network level	3G	Access emails
	Bluetooth	Share picture
	Wi-Fi	Connect to a Wi-Fi network
Machine level	CPU	16% CPU is in use
	Memory	12M Memory is allocated
	Battery	An application consumes 1% of the battery

3. Feasibility of host-based Behavioural Profiling

When looking to develop an IDS for a mobile device, the traditional network-based approaches are infeasible given the various networking technologies a single device is able to use and the differing stakeholders that own them. Therefore a host-based approach must be considered. Given the difficulty of establishing signatures in the first instance [12], and their inability to detect unknown attacks, a profiling was taken. However, little literature to date has tested the discriminative nature of service utilisation. Building upon the taxonomy identity in Table 1, a series of experiments have been conducted within each category or level: application, network and machine.

3.1. Experimental Procedure

An MIT Reality dataset was utilised. The dataset contained 94 participants' mobile device activities recorded from September 2004 to June 2005 [13]. The data was collected from the Nokia 6600 phone which was preinstalled with automatic logging software.

Table 2. The MIT Reality dataset

Activity	Number Of Logs	Information Contains
Application	662393	Application name, date and time of usage
Bluetooth scanning	1994186	Date, time of each scan along and individual device's MAC address
Charge	11506	Date and time when the mobile is in charge
Device usage	574788	Date and time the mobile has been in use
On	13012	Date and time when the phone is turned on
SMS	5607	Date, time and number of texting
Voice	54440	Date, time, number of calling and duration

As shown in Table 2, the dataset contains a rich volume of information which covers all the levels of mobile device usage. The experiment analysed the telephony, device usage, and Bluetooth scan activities; as representative of application level, machine, and network levels.

Telephony service was the first service invented for the mobile device. People use it to communicate with other people over a voice channel. The telephony service still dominates the mobile market along with increasing revenues across the globe [14]. The prior literature shows that the calling behaviour has been studied a number of times over the telecommunication service provider's network environment and it can be used to discriminate users. However, within the mobile host environment, the calling features have changed slightly, such as the IMSI can not be utilised anymore. Hence, it is important to establish whether the calling features still remain a positive attribute that can be used within a host-based environment.

Once the mobile device is in use, it becomes active; otherwise it may be either idle or switched off. When the mobile device is in the active mode, the following three scenarios would happen: a) the user views whatever information appears on the home screen, but does not interact with any applications; b) the user utilises one application, then sends the device to idle mode; c) the user uses more than one application to perform a task over one active session. For example, the user takes a photograph, views it, and emails it to a friend over a Wi-Fi connection. Whilst the example shows that the user utilises at least three applications to perform one big task over an active session, this particular experiment is simply focussed upon whether the device is in use and how unique and discriminative this information is.

Bluetooth is one of the short range networking technologies employed by the mobile device to communicate with nearby Bluetooth enabled devices. In order to do this, the mobile device has to scan nearby Bluetooth enabled device. Each scan may come up with a list of devices. Each device has a unique MAC address. Given the nature of a Personal Area Network (PAN) certain Bluetooth MAC address(es) may keep showing up on the scan list. For example, a user has a Bluetooth enabled headset, so its MAC address should appear on the Bluetooth scan list. Therefore it is possible to hypothesise, that a mobile device will encounter a familiar set of MAC addresses during normal activity – particularly within home and work environments. By learning those familiar Bluetooth MAC addresses, certain locations and potential trust can be established.

For data processing reasons, the experiment employed the first 30 users' activities over the first 10-month period. For each experiment however, only one month's activities were extracted for each individual activity in order to minimise any resulting inaccuracy, as it is likely that user's behaviour could change over time [15]. Template renewal or refresh is something that will be tackled once the feasibility of such an approach is proven. A series of iterative experiments were conducted across the three activities and complete time period.

4. Result and Discussion

4.1. Telephony

Table 3 shows the experimental results for the first 30 users one month's calling behaviour. Five calling features were utilised: the calling number, the day of calling, the time of calling, the duration of the conversation, and the weekday. The weekday feature was calculated by using the day feature; as people's activity on different weekdays could be different [4] [12]. A Radial Basis Network (RBF) was utilised in favour of other approaches given its previous success in [4] [7]. The configuration of which was iteratively modified to optimise performance. By using all five features, the best average Equal Error Rate (EER) achieved is 15.6% and it was achieved by using 150 neurons. Apart from the calling number, every other feature was removed from the neural network configuration in turn to understand the value that feature had upon performance. The best average EER was 13.5% and this was achieved by using 125 neurons with number of calling, the day, weekday, and duration. By using number of calling, time of calling, weekday and duration, the system got the highest average EER of 17.7%.

Table 3. Experimental result on calling

Neurons	Features	Average EER	Best user
150	Number, day, time, week, duration	15.6%	0%
130	Number, time, week, duration	17.7%	7.1%
125	Number, day, week, duration	13.5%	0%
135	Number, day, time, duration	13.6%	0%
140	Number, day, time, week	15.4%	0%

As shown in Table 3, the overall result for calling behaviour is positive – remembering the nature of this type of profiling is unlikely to result in EER in the same order of magnitude as physiological biometrics. As the number of features decreases, the number of required neurons also decreases; indicating that proper selection of the strong and positive features would save a significant amount of computing power. This is especially important in the mobile device environment: fast, accurate detection by using minimal computer power.

4.2. Device Usage

The device usage behaviour study also employed the first 30 users' information from the MIT Reality dataset. For the active behaviour, the following features were extracted from the dataset: the day, time, duration and weekday. Within table 4, the best average EER is 35.1% and this was achieved by using 5 neurons with the time, day, duration and weekday. The best individual user EER is 1% by using 7 neurons in the RBF neural network with the day, duration and weekday features. Interestingly, with the same neuron network configuration, 43% of the whole population achieved less than 30% of the EER, although majority of them have an EER in the region of 20%-30%.

Table 4. Experimental results on active

Neurons	Features	Average EER	Best user	Proportion of users EER<30%
5	Time, day, duration, weekday	35.1%	3.87%	36.7%
7	Time, day, duration	35.8%	3.82%	40%
7	Day, duration, weekday	36.2%	1%	43%
5	Time, day, weekday	36.4%	3.1%	33.3%

As there is no indication that what purpose the device has been used for, only knowing a usage occurred, the usability for distinct mobile users reduces significantly. However, this could be improved by knowing what has happened during the active duration: such as, one text message was sent. Moreover, the result does indicate that device usage can be used for identifying a subset from the entire mobile population; as at least 1/3 of the users have an EER rate less than 30%.

4.3. Bluetooth Scan

As the mobile device's Bluetooth scan performs passively every 5 minutes, a huge amount of information was available for processing. Given the repeated nature of the scans, samples may keep reappearing if the user stays in one location for a while, for example watching a film in the cinema or taking a lecture in the classroom. As a result, the experiment employed the first 30 users' Bluetooth scans which performed at 10 o'clock each day. However, due to the aforementioned restriction, only the MAC address, the day, and the week features were extracted from the sub dataset. Table 5 describes the experimental result on the Bluetooth scanning activities. By using 20 neurons with the MAC address and the day as the inputs, the RBF neural network achieved the best average EER of 35.7%. By using the same configuration, 30% of the experiment users have less than 30% EER. For the best individual user's EER, 0% was achieved in both RBF neural configurations.

Table 5. Experimental results on Bluetooth scanning

Neurons	Features	Average EER	Best user	Proportion of users EER<30%
15	MAC address, day, week	36.1%	0%	26.7%
20	MAC address, day	35.7%	0%	30%

Table 5 does show a positive set of results from Bluetooth scan behaviour, although the result is a little bit noisy. It may cause by the nature of Bluetooth scan behaviour, as the content of a Bluetooth scan list heavily relies on other Bluetooth enable devices. For example, in an office environment, a mobile user's Bluetooth scan list may contain colleagues' Bluetooth enabled device and a number Bluetooth enabled desktop PCs; as the colleagues come in and out the office, the user's Bluetooth scan list will change accordingly. The scan list may change slightly but within a familiar set of MAC addresses. Also, the experimental results show that a proportion of users' Bluetooth scanning behaviour are quite predictable as 30% of them have an EER less than 30%.

From the above three experiments, the positive results identify that the calling, device usage and Bluetooth scanning behaviours used to profile mobile users. However, the level of performance is such that no single feature could be utilised to make decisions over misuse – the inconvenience of being wrongly identified would be too high. This suggests that a new mobile IDS could have

a behaviour selector for each individual user to choose correct behaviour accordingly. Moreover, it can also be seen that the individual user's performance with each activity differs – thereby suggesting that an IDS system capable of weighting the input features on an individual user basis would be better suited to optimising overall performance. Finally, whilst individual results will go someway in understanding the legitimacy of a user, the combination or fusion of multiple inputs would only serve to support the decision making process [16, 17].

5. Host Based Multi-level Behaviour Profiling Mobile IDS Framework

With the aim of providing accurate and robust detection of misuse, a proposed framework is presented in Figure 1. The Host-based Multi-level Behaviour Profiling Mobile IDS framework is capable of processing multiple user activities from all levels of the taxonomy identified in Table 1 and intelligently interpreting the results to provide a more robust decision making process.

As shown in Figure 1, all the user's mobile behaviours can be used as the system input; the input can be one activity or the combination of multiple behaviours. For example: Wi-Fi activity from the network level. Also, the system can select a combination of multiple inputs; for example, when a user surfs the Internet, surfing features (explorer, web address, day and time of visiting) from the application level, network features (network type, number of data packets, and transmission rate) from the network level, and CPU usage from the machine level. As each individual user may have a different way to use the mobile device, therefore the system employs a Multi-Level Behaviour Selector to choose appropriate inputs accordingly. The selection process is carefully considered and the selection criteria are defined differently for individual behaviour. For example, the percentage of unique dialled numbers: when it is bigger than the threshold, the calling activity will be selected; as the user makes a unique set of calls, it is much easier to profile the user's behaviour. Another example is the frequency of application usage; when it is smaller than the threshold, that application's features will not be used as the input; as if an application is not regularly used, there will not be enough information to help the profile building. Also, as the user's behaviour may change over time, the Multi-Level Behaviour Selector will update the input selection accordingly.

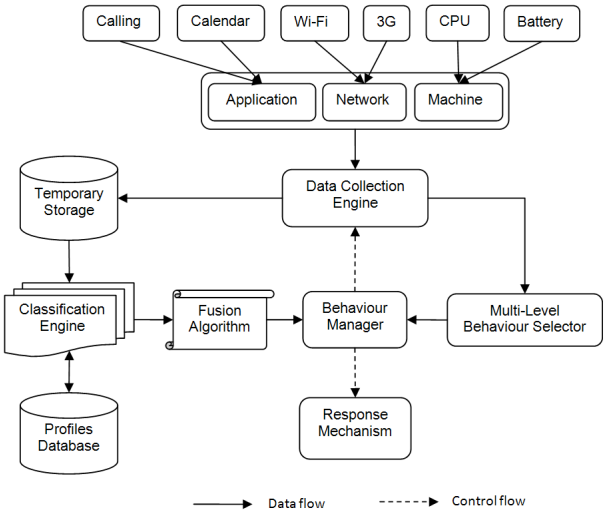


Fig. 1. Host based multi-level behaviour profiling mobile IDS framework

Following by the information provided by the Multi-Level Behaviour Selector, the Behaviour Manager sends a command to the Data Collection Engine to collects the user behaviour features accordingly. Depending on the selected inputs, the Classification Engine can use various classification methods to compare the current activity against the profile: such as neural networks, fusion functions, and decision trees. The result will be further processed by the Fusion Algorithm. The Fusion Algorithm calculates the weight for each activity as each behaviour has a different impact on the decision making; for example, a more regular used application will have more weight on the decision when compared with others. The Behaviour Manager then sends the decision to the Response Mechanism, such as launching antivirus software, restricting access to certain applications, or even locking down the mobile device.

As the Host based Multi-Level Behaviour Mobile IDS framework takes all the possible activities as the inputs, so it will provide full detection for all the mobile applications, the network connection and machine levels. Moreover, the framework will operate independently for each individual mobile user.

6. Conclusion

It is essential that new approaches are developed to enable real time detection of mobile misuse on both known and unknown threats. Given the personal nature of the mobile device, behavioural profiling provides an opportunity to closely map an individual's use of a device. The experiments have demonstrated that individual activities can indeed be profiled and used to identify legitimate and illegitimate use.

The strength of this identification however is highly variable between users with some experiencing very high

levels of classification and others not. Given this variability no single technology would be stable for uniform deployment but rather through the utilisation of multiple activities within an appropriately flexible and robust framework, a more secure yet convenient approach can be realised.

Future work will seek to identify further activities that can be used for classification. Focus will also be given to the theoretical and practical issues surrounding the proposed framework.

7. References

[1] Rao, J.R., Rohatgi, P., Scherzer, H., Tinguely, S.: Partitioning Attacks: Or How to Rapidly Clone Some GSM Cards. In: the 2002 IEEE Symposium on Security and Privacy, pp. 31--41. IEEE Computer Society, Washington, DC, USA (2002)

[2] Swami, Y. P.,Tschofenig, H.: Protecting mobile devices from TCP flooding attacks. In: Proceedings of first ACM/IEEE international workshop on Mobility in the evolving internet architecture, pp.63--68. ACM, New York (2006)

[3] Kaspersky Lab, http://www.viruslist.com/en/analysis?pubid=204792080, date of access: 02 February 2010.

[4] Li, F., Clarke, N.L., Papadaki, M.: Intrusion Detection System for Mobile Devices: Investigation on Calling Activity. In: Proceedings of the 8th Security Conference, April, Las Vegas, USA (2009)

[5] Gosset, P.:ASPeCT: Fraud Detection Concepts: Final Report. Doc Ref. AC095/VOD/W22/DS/P/18/1, (1998)

[6] Samfat, D., Molva, R.: IDAMN: an Intrusion Detection Architecture for Mobile Networks. In: IEEE Journal on Selected Areas in Communications, vol. 15, pp.1373--1380. IEEE (1997)

[7] Boukerche, A., Nitare, M.S.M.A.: Behavior-Based Intrusion Detection in Mobile Phone Systems. In: Journal of Parallel and Distributed Computing, vol. 62, Issue 9, pp. 1476-1490. Academic Press, Inc. Orlando, FL, USA (2002)

[8] Buschkes, R., Kesdogan, D., Reichl, P.: How to increase security in mobile networks by anomaly detection. In: proceedings of the 14th Annual Computer Security Applications Conference, pp. 3--12. IEEE Computer Society, Washington, DC, USA (1998)

[9] Sun, B., Chen, Z., Wang, R., Yu, F., Leung, V.C.M.: Towards adaptive anomaly detection in cellular mobile networks. In: the IEEE Consumer Communications and Networking Conference, 2006 (CCNC 2006), Vol. 2, pp. 666--670. IEEE (2006)

[10] Hall, J., Barbeau, M., Kranakis, E.: Anomaly-based intrusion detection using mobility profiles of public transportation users. In: the Proceeding of IEEE International Conference on Wireless And Mobile Computing, Networking And Communications, 2005 (WiMob'2005), vol. 2, pp. 17--24. IEEE (2005)

[11] Martin, T., Hsiao, M., Ha, D., Krishnaswami, J.: Denial-of-Service Attacks on Battery-powered Mobile Computers. In: Second IEEE International Conference on Pervasive Computing and Communications, pp. 309--318. IEEE Computer Society, Washington, DC, USA (2004)

[12] Jacoby, G.A., Hickman, T., Warders, S.P.: Gibraltar: A Mobile Host-Based Intrusion Protection System. In: Proceedings of the 2006 International Conference on Security & Management, pp.207--212, Las Vegas, Nevada, USA (2006)

[13] Eagle, N., Pentland, A., Lazer, D.: Inferring Social Network Structure using Mobile Phone Data. In: Proceedings of the National Academy of Sciences (PNAS), vol 106, pp.15274--15278. PNAS (2009)

[14] Ofcom, http://www.ofcom.org.uk/research/cm/cmr09/cmr09.pdf, date accessed: 15 February 2010

[15] Biermanna, E., Cloeteb, E., Venterc, L.M.: A comparison of Intrusion Detection systems. In: Computer & Security, Vol 20, pp.676--683. Elsevier (2001)

[16] Lerouge, E., Moreau, Y., Verrelst, H., Vandewalle, J., Stoermann, C., Gosset, P., Burge, P.: Detection and management of fraud in UMTS networks. In: Proceeding of the Third International Conference on The Practical Application of Knowledge Discovery and Data Mining (PADD99), pp. 127--148. (1999)

[17] Furnell, S., Clarke, N., Karatzouni, S.: Beyond the PIN: Enhancing user authentication for mobile devices. In: Computer Fraud & Security, Vol 2008, Issue 8, pp. 12--17. Elsevier (2008)

Intrusion Detection System for Mobile Devices: Investigation on Calling Activity

Fudong Li, Nathan Clarke and Maria Papadaki

Centre for Information Security & Network Research, University of Plymouth, Plymouth, United Kingdom
info@cisnr.org

Abstract

In recent years, an increasing focus has been given to the development of security controls to counter current existing mobile security threats; such as Anti-Virus and firewalls, which are both now commercially available. Nevertheless, with the increasing functionality of mobile devices, a need exists for more sophisticated security controls and research is focusing upon other security controls like Intrusion Detection Systems (IDS). Indeed, a number of research efforts on IDS for the mobile device have already been given. However, those mobile IDSs are designed to detect particular security threats related to individual service (e.g. telephony). The aims of this paper are firstly to identify the need for a novel mobile IDS which can provide detection for multiple services and support multi-networks simultaneously; and to identify the positive calling activities' features to discriminate users. This paper begins with investigating the current research on mobile IDS with a view of examining the positive and negative aspects. The paper then processes to describe an experimental study on user's calling activity. The experiment result shows that within the host environment, the number of calling, the time of calling and the duration of calling can be used to discriminate legitimate users and attackers. The paper will conclude with the future research for the mobile IDS.

Keywords: *Intrusion Detection System, mobile devices*

1. Introduction

Currently, the mobile device has become a ubiquitous computing device. It has experienced an evolutionary shift from a purely telephony based handset into a modern computing device with multiple variants, such as the Smartphone, PDA (Personal Digital Assistant), and Ultra-mobile PCs. For the mobile telephone alone, it has over 3.2 billion subscribers around the world (GSM Association, 2008). Indeed, a large number of developed countries are experiencing well in excess of 100% market penetration (ITU, 2007). The modern mobile device is capable of providing a wide range of services over several network connections and is able to store a broad range of information from business to personal data. As a result, many people rely on those services and information to complete their business and personal tasks. Such tasks can include email accessing via wireless network, online shopping through the 3G network, sharing pictures over the Bluetooth connection, and reading word documents. However, those activities can contain sensitive data related to the business and personal private information.

The mobile device faces several security threats. Traditionally, service fraud, handsets being lost or stolen and SIM (Subscriber Identity Module) card cloning were three major

security threats (BBC, 2005; Metropolitan Police Service, 2008; Rao *et al*, 2002). According to the Forum for International Irregular Network Access, the service fraud is estimated to cost telecom service providers $55 billion every year around the world (European Communications, 2005). Recently, with the evolution of the mobile device, it is also experiencing several new security threats, such as malware, information disclosure, and Denial of Service (DoS) (Muir, 2003; Swami and Tschofenig, 2006; Stajano and Anderson, 1999). Although these new threats were discovered a few years ago, the number of incidents grows significantly every year (McAfee, 2007). For instance, there were already more than 100 variants of mobile malware in existence at the end of 2005 (IT-Observer, 2007). To counter those security threats, various mobile security projects have been proposed and developed; such as antivirus, biometrics, encryption and firewalls (F-Secure, 2008; Clarke and Furnell, 2007; Check point, 2008; Anthasoft, 2008). This reveals that a real lack of effective information security still exists (Perelson and Botha, 2004).

Due to the incompatibility of the existing IDS with the mobile device, research for the mobile IDS started in the middle of 1990s. Early mobile IDS research developed mechanisms of detecting traditional attacks; such as the European project Advanced Security for Personal Communications (ASPeCT) for detecting telephony service fraud (Gosset, 1998). More recent mobile IDS studies have focussed upon detecting newer attacks; i.e. the battery based mobile IDS and the mobile agent based IDS (Jacoby *et al*, 2006; Kannadiga *et al*, 2005). However, the amount of mobile IDS research is significantly smaller compared to other aforementioned mobile security projects. Moreover, those existing mobile IDSs were designed to detect the individual security threats: telephony based mobile IDSs only detect telephony service fraud; battery based mobile IDSs only detect battery attacks. Therefore, none of these mobile IDSs is capable of offering the comprehensive detection for the services running on the modern mobile devices.

This paper begins with introducing the concept of the modern mobile device, the threats associated with the device, and general security controls. The main discussion starts with presenting the history of the traditional IDS and follows by a critique of the mobile IDS: their different variants and their working principles, performance, and advantages and disadvantages. In section 3, a behaviour and host based mobile IDS is proposed. The paper describes a research programme underway to design, develop and evaluate a novel mobile IDS. The paper then proceeds to present some initial experimental results and concludes with highlighting the future work.

2. Mobile Intrusion Detection System

In 1980, the first notion of intrusion detection was created in Anderson's paper "Computer Security Threat Monitoring and Surveillance": by using mainframe audit trails to trace misuse actions and to understand users' behaviour in the computer system (Anderson, 1980). In 1987, Denning proposed the seminal work: "An Intrusion Detection Model", which identified basic IDS components and their functionalities (Denning, 1987). Since then, a considerable amount of IDS research has been carried out and a range of prototypes and commercial products were developed (Stefan, 2000). However,

because of the unique characteristics that the mobile device has: low processing power, small storage space, differing network accesses and a unique set of services; these existing IDSs are not suitable to provide detections for the mobile device. Host based IDSs are too complicated for mobile devices to handle; network based IDSs can only monitor a single network at any one time.

The research for mobile IDS started around 1995 with preliminary focus upon detecting telephony service fraud. Telephony service fraud occurs when the mobile device is lost or stolen, or the SIM card is cloned. In the worst case, the owner would not notice the attack until the end of the billing month. At that moment, significant financial damages would have been made for both the owner and the telecom service company. By monitoring users' calling behaviour, the aforementioned attacks can be detected (Samfat and Molv, 1997). With increasing computational power, the mobile device offers more services: such as, accessing emails, and transferring data file over different network connections. However, those services raise new security risks: malware and DoS attacks. As a result, several signature based mobile IDSs have been developed.

2.1. Behaviour based mobile IDS

The modern mobile device provides a wide range of services, however, the way people use those services can be completely different. As a result, people's behaviour on their mobile device can be arguably distinguished. Indeed, the user's calling activity, migration mobility activity and migration itinerary activity have already been utilised to detect telephony service fraud, SIM card cloning and lost or stolen of the device. To date, all behaviour based mobile IDSs are network based systems; as user's behaviours are obtained and monitored by network services providers.

2.1.1. Telephony based mobile IDS

The telephony based mobile IDS monitors user's calling attributes (e.g. international Mobile Subscriber Identity (IMSI), start date of call, start time of call, duration of call, dialled telephone number and National or International call) to detect service fraud, SIM card cloning, and lost or stolen of devices (Moreau *et al*, 1997). By using the combination of those attributes, a historical profile can be acquired. If the deviation between the current calling session and the historical profile exceeds a threshold, an intrusion is identified. There are several telephony based mobile IDSs existing, and they can be separated by their pattern classification techniques. For example, Stormann (1997), and Boukerche and Notare (2002) utilised a supervised method; and Samfat and Molva (1997), and Alves *et al* (2006) employed an unsupervised method. Generally speaking, telephony based mobile IDSs have a good system performance: high detection rate and low false alarm rate. In addition, as the detection process is carried out by the network operator, there is no restriction on the mobile device. The major disadvantage is that they only focused upon telephony services and can not provide any detection for other network services. Moreover, those systems can not provide any detection for data related attacks.

2.1.2. Migration mobility based mobile IDS

By calculating the chance of a mobile user travelling from one mobile cell to another, the migration mobility based mobile IDSs can also detect traditional attacks. If the calculated result exceeds the threshold, a possible intrusion occurs. There are several mobility based mobile IDSs: Buschkes *et al* 1998, Sun *et al* 2004, and Sun *et al* 2006. Among those systems, Sun *et al* 2006 has the best system performance. It employed several methods to achieve this: the high order Markov chain model, the Exponentially Weighted Moving Average Model and the Shannon's entropy theory. As a result, the system has a constantly updated profile, and a suitable threshold. Furthermore, as the user's activities could be extremely different over the weekdays and weekends, two separated profiles were used according to those two periods. From their simulation result, it shows that the system's best detection rate is around 94% and the lowest false positive rate is around 5% when the user travels at the speed of 60 miles per hour. However, the performance decreases dramatically when the user travels on foot. The main advantage for those systems is they are suitable for those long distance regular travellers who spend a lot of time on travelling. However, the number of those travellers is reasonably small within the mobile users' population. Furthermore, those systems can not provide detection for malware and data related attacks.

2.1.3. Migration itinerary based mobile IDS

Whilst similar to migration mobility based mobile IDS, the migration itinerary based mobile IDS also monitors cells to detect traditional attacks. However, instead of only monitoring one cell each time, the migration itinerary based mobile monitors all the cells the user covers from one location to another. People always have the destination in their mind when they travel. Therefore, certain routes will be chosen as regular or favourite routes. As a result, the probability of the mobile user travels over those routes is much higher than when they travel through other routes. To extend this, when an attacker carries other people's mobile device, the route he is going to cover will be probably different in comparison with the owner's routes. In 2005, Hall *et al* have published a paper on using public transportation user's itinerary profile to detect intrusions via an instance based learning pattern classification technique (Hall *et al*, 2005). However, their simulation result was not particularly promising. In addition, the system could only monitor those mobile users who take the public transport system. Moreover, these systems suffer the same problem as the mobility based mobile IDS does: they can not provide detection for malware and data related attacks.

2.1.4. Comparison on behaviour based Mobile IDS

Table 1 illustrates the comparison for all aforementioned behaviour based mobile IDSs. Generally speaking, telephony based mobile IDSs have a better Detection Rate (DR) and False Alarm Rate (FAR) than the migration activity based mobile IDSs do. In addition, the telephony based mobile IDS provides the detection for more users than the migration activity based mobile IDS could. However, the migration activity based mobile IDS does have the potential ability to provide the detection for all services provided by the service provider. The advantages for behaviour based mobile IDSs are: as the detection process is carried out by the services provider, there is no overhead or requirement for the mobile device. Also, those IDSs can identify the telephony service fraud, SIM card cloning and

the lost or stolen of devices. On the other hand, those systems can not detect any other service frauds. Also they can rarely provide any detection against following mobile security threats: malware, information leakage, DoS, and data modification. Furthermore, the mobile user's privacy could also be an issue.

Name	Behaviour	Pattern classification model	DR	FAR
Samfat and Molva, 1997	Itinerary	Mathematical formula	82.5%	4%
	Calls	Mathematical formula	80%	3%
Boukerche and Notare, 2002	Calls	RBF neural network model	97.5%	4.2%
Stormann, 1997	Calls	Rule based	99%	24%
Alves *et al*, 2006	Calls	Distance-based and clustering	91%	NA
Buschkes *et al* 1998	Mobility	Bayes decision rule	87.5%	NA
Sun *et al* 2004	Mobility	High order Markov model	87.5%	15%
Sun *et al* 2006	Mobility	High order Markov model	89%	13%
Hall *et al*, 2005	Itinerary	Instance based learning	50%	50%

Table 1: Comparison for the Behaviour based Mobile IDS

2.2. Signature based mobile IDS

The research on the signature based mobile IDS started in early 2000. The main aim of developing the signature based mobile IDS was to detect malware and DoS attacks for the mobile device. At present, there are four prototype signature based mobile IDSs and they are categorised into two groups: the battery based mobile IDS and the mobile agent based mobile IDS.

2.2.1. Battery based mobile IDS

It is widely recognised that the battery plays a key role in a mobile device, to provide continuous services to the user. If the attacker is able to drain the battery, the mobile device's servicing time will be reduced. Therefore, attacking the battery is a major threat for the mobile device's availability. In order to counter battery attacks, three studies based on analysing the battery activities have been conducted: Power Secure Architecture, Battery Based Intrusion Detection Model and Gibraltar (Martin *et al*, 2004; Jacoby *et al*, 2004; Jacoby *et al*, 2006). These systems all work in a similar fashion. Each mobile application consumes unique power, so does malware. As a result, by analysing current activities, various signatures for either legitimate applications or malicious codes can be obtained. The battery based mobile IDS continually monitors battery activities and compares them with its signatures to detect any anomalies. The advantage for these systems is that by monitoring battery activities, malware attacks and attacks on the battery can be detected. However, obtaining malware's signatures can be a very difficult task.

2.2.2. Mobile agent based mobile IDS

In 2005, Kannadiga *et al* proposed a mobile agent based IDS for the pervasive computing environments (Kannadiga *et al*, 2005). In a pervasive computing environment, various mobile devices can be found: such as mobile phones and PDAs. Their mobile IDS

employs the mobile agent, by moving it from one mobile device to another within the network, collecting information (such as application log files) from mobile devices, to indentify malicious activities on each mobile device. It is reasonable to use mobile agents to detect intrusion for those low computing powered mobile devices. In addition, by knowing the attack on the mobile host, the network threat can also be identified. The major drawback is that signatures are created by monitoring malicious activities on networked static hosts (i.e. virus on the desktop PC); therefore those signatures are more related to static hosts, rather than for mobile devices. As a result, mobile malwares attacks can not be detected. Also, the mobile device can be not protected when it leaves the network.

2.2.3. Comparison on signature based mobile IDS

Table 2 illustrates the comparison for signature based mobile IDSs. For the battery based mobile IDS, their sensors are all allocated on mobile devices' battery. For the mobile agent based mobile IDS, the mobile agent is the sensor. The correlation process is carried out in three different ways: Martin *et al* 2004 is done on the mobile device, Kannadiga *et al* 2005 is executed on the network based server, and Jacoby *et al* 2004 and Jacoby *et al* 2006 can be carried out both locally or on the network based server. Various approaches have been taken to obtain the signature: Martin *et al*, 2004 uses the legitimate services as the signatures, any process' signature not in the database can be identified as malicious. The signature database is reasonably small as the number of legitimate mobile services is currently limited. Both Jacoby *et al*, 2004 and Jacoby *et al*, 2006 employed the most popular network relate attacks as the attacking signature. However, the database is pretty small when compared with the number of existing attacks; moreover, as those network attacks are found in the traditional desktop environment, they are less relevant for the mobile device. The Kannadiga *et al* 2005 also suffers this problem as their attacking signatures are gathered by the static agent from local hosts. The major break through for the signature based mobile IDS is that it can possibly detect the malware and battery attacks. On the other side, it can not provide any protection against data related attacks, and service fraud. Also, obtaining accurate and a wide range of signatures is a very challenging task in practice.

Name	Sensor location	Correlation location	Signatures types	Attacks can be detected
Martin *et al*, 2004	Battery	Host	Legitimate Services	Malware and Power attacks
Jacoby *et al*, 2004	Battery	Host and network	Common network attacks	Common network attacks
Jacoby *et al*, 2006	Battery	Host and network	Common network attacks	Common network attacks
Kannadiga *et al*, 2005	Mobile Agent	Network server	Signatures from the desktop environment	Network related attack

Table 2: Comparison for the Signature based Mobile IDS

2.3. Summary of current Mobile IDS

The behaviour based mobile IDS is able to detect attacks on telephony service fraud. The signature based mobile IDS could identify possible malware and DoS attacks. However, both types fail to provide any detection for other services and network connections as shown in Table 3. This is really worrying as people use these services on the mobile device on a daily basis. As a result, a mobile IDS which can offer the detection for a wider range of services and connections on the mobile device is certainly needed.

	Services				Networks			
	Call\SMS	Internet	Email	Data storage	Cellular network	WiFi	Bluetooth	Cable
Boukerche and Notare, 2002	Y	-	-	-	Y	-	-	-
Sun *et al* 2006	Y	-	-	-	Y	-	-	-
Samfat and Molva, 1997	Y	-	-	-	Y	-	-	-
Martin *et al*, 2004	-	-	-	-	-	-	-	-
Jacoby *et al*, 2006	-	-	-	-	-	Y	-	-
Kannadiga *et al*, 2005	-	-	-	-	-	Y	-	-

Table 3: Mobile IDS VS mobile device's services and networks

3. Experimental studies on a behaviour & host based mobile IDS

As mentioned previously, the usage of the mobile device has changed dramatically. Also, as shown in section two, current existing mobile IDSs can not provide continuous detection for all the services the mobile device offers, along with the information stored on the device. Given the specific requirements, a *Behaviour and Host based Mobile IDS* is proposed. There are several reasons behind this proposal: the behaviour and host based mobile IDS can provide detection for services running on the mobile device against the service fraud, data disclosure and modification attacks. Also, the host based mobile IDS can monitor all network connections which a single network based system is unable to achieve.

It is arguable that people's behaviour on the mobile device can be different due to the purpose of the usage. For example, a user accesses his mobile calendar service to find out what his schedule looks like, the features related to this behaviour can be the time of accessing (7.15 AM), the duration of accessing (1 minutes) and the day of accessing (Monday). However, when an intruder accesses the same calendar service, the intruder may choose a time which the owner would not use the device such as 3 AM in the morning and the duration of accessing should be much longer such as 5 minutes as the intruder wants to explore as much information as possible. As a result, various user's behaviours within the mobile platform should be studied to identify positive behavioural features that could be utilised to discriminate between legitimate users and intruders. In this paper, an experiment study on user's calling behaviour is presented on the following section.

3.1. Telephony based experiment

The prior literature shows that the calling behaviour has been studied a number of times over the telecom service provider's network environment and its features can be used to discriminate users. However, within the mobile host environment, the number of calling behaviour's features reduced significantly: from 6 features for the network based environment down to 3 features within the host platform. According to the Ofcom's "The International Communication Market 2007" research report, the calling service still predominate the mobile communication market (Ofcom, 2007). As taken those two points of views into consideration, the research started with identifying positive calling behaviour's features within the host environment.

The experiment employed 45 participants who had more than four month's calling activity from the existing MIT Reality dataset (MIT, 2008). As the condition is under the host environment, only the *number of dialling*, the *calling time*, and the *duration of the conversation* were extracted from the dataset as these can be established by the mobile host. The dataset for those 45 participants contains a total 15,702 calls. In addition, those 15,702 calls have been formed two sub-datasets: weekdays and weekends as people's activities can be extremely different over those two periods. The datasets were divided into two: the first half was used for training the classifier and the second half was used for the validation. Two neural networks (Feed-Forward Multi-Layered Perceptron Neural Network and Radial Basis Function Neural Network) with a total of 99 configurations were chosen (81 for FF MLP and 18 for RBF).

Table 4 demonstrates a summary of best sets of experiment results with three groups of inputs over three sets of time periods by using various FF MLP Neural network configurations. The results clearly shows that by using the number of calling alone as the input, the FFMLP neural network achieved the lowest Equal Error Rates (EER) with 8.71%, 7.05% and 8.57% for *weekdays*, *weekends* and *weekly* accordingly. With the number of the inputs increases, the FFMLP neural network's performance gets worse. The results indicate that by adding the *time of calling* and the *duration of calling*, those two features made more impact for the *weekends*' performance than they did for the *weekdays*'.

Input(s)/ Features	Periods	Neurons	Epochs	EER
Number of calling only	weekdays	150	150	8.71%
	weekends	150	100	7.05%
	weekly	150	50	8.57%
Number of calling, and time of calling	weekdays	50	150	21.61%
	weekends	50	150	25.80%
	weekly	100	50	21.96%
Number, Time of calling, and duration of calling	weekdays	50	100	22.58%
	weekends	50	100	25.44%
	weekly	50	100	21.03%

Table 4: Experiment result on FFMLP Neural network

Table 5 illustrates all the experiment results by using RBF neural network. Due to too much input data, it is not feasible for the RBF neural network to simulate the weekly situation. In order to compare the performance with the FF MLP neural network, same set of maximum number of neuron has been chosen for the RBF neural networks. The result demonstrates that by using only the *number of calling* as the input and maximum 150 neurons, the RBF neural network obtained the best performance with the EER 6.95% and 6.21% for *weekdays* and *weekends*. With increasing number of inputs, the RBF neural network's performance gets worse; however, the RBF neural network's EER only grew around twice comparing with three times for the FF MLP neural network did. Also when the number of inputs increases, they have more impact for the *weekends*' performance than they do for the *weekdays*'; this pattern is also shown by the FF MLP neural network in Table 4.

Input(s)/Feature(s)	Periods	Neurons		
		50	100	150
Number of calling only	Weekdays	8.12%	7.55%	6.95%
	Weekends	6.80%	6.30%	6.21%
Number of calling, And time of calling	Weekdays	11.82%	9.66%	9.53%
	Weekends	14.23%	12.86%	12.09%
Number of calling, Time of calling, and duration of calling	Weekdays	12.60%	11.24%	10.95%
	Weekends	16.32%	15.44%	16.67%

Table 5: Experiment result on RBF neural network

From the above two set results, they show that by using the *number of calling* alone, the best simulation results were obtained. With the number of inputs increases, the overall performance decreases. This shows that the *number of calling* is a positive discriminate feature and the *time of calling* and the *duration of calling* are having a negative discriminative effect for this particular dataset. By using number of calling only, the *weekends*' performance is better than *weekdays*', this may because over the weekends less numbers have been dialled; or the user may only contact their family and friends over the weekend. With the number of inputs increases, the neural networks got better performance during the weekdays than they do over the weekends. This shows that people may do regular tasks during weekdays and their weekends' activities are much more random.

The experiment results are what would be expected as users regularly call a subset of people. However, using only *number of calling* feature, a category of misuse is missed when people do call the same number. As a result, more analysis has been made on those 45 individual users. Within those 45 users, three groups users have been found: within the first group, 12 users never share any same dialled number with any one; within the second group, 13 users shares between a minimum of 6 and a maximum of 18 dialled numbers between minimum 2 users and maximum 8 users within those 13 users; and for the third group, users only share a few number of same dialled numbers among one or two other users. This reviews that more than 2/3 of users with the 45 users' dataset do not share large amount dialled number with others. The hypotheses is that if the number has been dialled before, the *time of calling* and the *duration of calling* would play positive

discriminate roles to identify the different mobile users. Otherwise, they play negative discriminate roles in the identification process.

More experiments have been carried out to test the hypotheses to identify roles the *time of calling* and the *duration of calling* play for different types of users by using RBF neural network. The reasons for employing the RBF neural network are: simulation results from Table 4 and Table 5 show that the RBF neural network outperformance the FFMLP neural network; similar conclusion has also been found by previous study (Boukerche and Notare, 2002); moreover, during the experiment, the RBF neural network was much more stable comparing with the FFMLP neural network was.

Table 6 demonstrates the experiment result on the first group users which contains total 2811 calls. The best performance is achieved by using the number of calling only with the EER of 3.24%, 3.31% and 4.30% for *weekdays*, *weekends* and *weekly* accordingly. Those results are even better than the results from Table 5. With the number of inputs increases, the performance gets worse and worse. This is due those user do not share any dialled number, by adding more inputs, it will only confuse the neural network and get poorer performance.

Neurons	Input(s)	EER(weekdays)	EER(weekends)	EER(weekly)
50	1*	3.24%	4.60%	4.30%
	2*	5.93%	14.13%	8.10%
	3*	8.50%	15.39%	8.45%
100	1*	3.33%	3.31%	4.74%
	2*	6.64%	11.17%	7.34%
	3*	7.59%	14.60%	8.00%
150	1*	3.33%	3.31%	4.60%
	2*	5.91%	12.11%	7.53%
	3*	8.22%	14.89%	8.32%

Table 6: Experiment result on first group users

1* number of calling 2*: number of calling, and time of calling 3*: number of calling, time of calling and duration of calling

Table 7 illustrates the experiment result on the second group users who do share a number of same dialled numbers with total number of 3966 calls within this dataset. Interesting results are shown by Table 7 as by using only the *number of calling* the neural network has the worst performance. By adding the *time of calling* to the inputs, the neural network's performance improved significantly for all the network configurations; by adding the *duration of calling* to the inputs, the neural network's performance improved slightly for most configurations. This reviews that both of the *time of calling* and the *duration of calling* play a positive role when the number has been dialled before and the *time of calling* has a stronger impact for the performance than the *duration of calling* does. Generally speaking, by using three inputs together, the neural network's performance is better than by *using the number of calling* only, and is worse than by using the *time of calling* and the *number of calling* together.

Neurons	Inputs	EER(weekdays)	EER(weekends)	EER(weekly)
50	$1^{\#}$	20.27%	21.58%	20.70%
	$2^{\#}$	18.35%	18.64%	16.92%
	$3^{\#}$	19.32%	21.31%	19.39%
	$4^{\#}$	19.65%	21.91%	17.41%
100	$1^{\#}$	18.05%	22.17%	20.75%
	$2^{\#}$	17.52%	18.48%	16.17%
	$3^{\#}$	19.35%	21.24%	18.82%
	$4^{\#}$	17.04%	21.15%	17.12%
150	$1^{\#}$	17.78%	22.18%	18.90%
	$2^{\#}$	15.49%	18.18%	16.08%
	$3^{\#}$	19.83%	20.71%	18.62%
	$4^{\#}$	17.74%	21.43%	17.15%

Table 7: Experiment result on second group users

$1^{\#}$: number of calling $2^{\#}$: time of calling and number of calling, $3^{\#}$ number of calling and the duration of calling and $4^{\#}$: number of calling, time of calling and duration of calling.

From the above experiment results, it shows that the *number of calling*, the *time of calling* and the *duration of calling* could all play the positive role to discriminate users. However, the *time of calling* and the *duration of calling* treated differently depend on whether the *number of calling* has been dialled before. If the number has never been dialled before, by adding the *time of calling* and the *duration of calling* can only decrease the classifier's performance. For the number has been dialled before, the performance for the classifier improves by adding the *time of calling* and/or the *duration of calling*; this will help the classifier to detect the data related attacks, as data can be viewed by anyone, however, the time or the duration for the attacker to access the same file may be different with the legitimate users.

4. Conclusion

In this paper, a comprehensive literature view on the mobile IDS has been given. It is clear that people use the mobile device to complete both business and personal work on a daily basis, and an increasing range of threats exist. By studying the positive and negative aspect of current mobile IDSs, a new mobile IDS which can offer the detection to cover a wider range of services is required.

The experimental results show that three positive calling features have been found to discriminate users within a mobile host platform. In order to support the development for a *Behaviour & Host based Mobile IDS*, other user's behavioural features should be studied. The results of these experiments will inform the design of proposed mobile IDS that is capable of detecting and acting upon a wide range of threats in an efficient and effective manner.

5. References

Anderson, J.P. (1980) "Computer Security Threat Monitoring and Surveillance", available at: http://seclab.cs.ucdavis.edu/projects/history/papers/ande80.pdf, accessed: 26 November 2007

Anthasoft (2008) "AnthaFirewall", available at: http://www.anthasoft.com/anthafirewall-firewall-for-mobile-device.php accessed: 26 August 2008

BBC (2005) "Cabs collect mountain of mobiles", available at: http://news.bbc.co.uk/1/hi/technology/4201915.stm date accessed: 25 August 2008

Boukerche, A. and Nitare, M.S.M.A. (2002) "Behavior-Based Intrusion Detection in Mobile Phone Systems", *Journal of Parallel and Distributed Computing*, Vol:62, pp. 1476-1490

Buschkes, R., Kesdogan, D. and Reichl, P. (1998) "How to increase security in mobile networks by anomaly detection", *proceedings of the 14th Annual Computer Security Applications Conference*, pp 23-12

Check Point (2008) "Pointsec Mobile", available at: http://www.checkpoint.com/products/datasecurity/mobile/ date accessed: 01 September 2008

Clarke, NL and Furnell SM (2007) "Advanced user authentication for mobile devices", *Computers & Security*, Vol.26, no.2, pp109-119

Denning, D.E. (1987) "An intrusion-detection model", *IEEE Transactions on Software Engineering*, Volume: SE-13, Issue: 2, pp. 222- 232, ISSN: 0098-5589

European Communications (2005) "Fraud management", available at: http://www.eurocomms.com/features/11905/Fraud_management.html, date accessed: 15 August 2008

F-Secure (2008) "F-Secure Mobile Anti-Virus" available at: http://mobile.f-secure.com/ date accessed: 01 September 2008

Gosset, P (Editor). (1998) "ASPeCT: Fraud Detection Concepts: Final Report", Doc Ref. AC095/VOD/W22/DS/P/18/1, Jan 1998.

GSM Association (2008), available at: http://www.gsmworld.com/index.shtml, date accessed: 21 February 2008

Hall, J., Barbeau, M. and Kranakis, E. (2005) "Anomaly-based intrusion detection using mobility profiles of public transportation users", *the Proceeding of IEEE International Conference on Wireless And Mobile Computing, Networking And Communications*, 2005 (WiMob'2005), Vol: 2, pp: 17- 24, ISBN: 0-7803-9181-0

International Telecommunication Union (ITU) (2007) "ITU World Telecommunication/ICT Indicators Database", available at: http://www.itu.int/ITU-D/icteye/Reporting/ShowReportFrame.aspx?ReportName=/WTI/BasicIndicatorsPublic&RP_intYear=2007&RP_intLanguageID=1, date accessed: 14 August 2008

IT-Observer (2007) "2005: Viruses, Phishing and Mobile Phone Malware", available at: http://www.it-observer.com/articles.php?id=971, date accessed: 13 November 2007

Jacoby, G.A., Hickman, T. and Warders, S.P. (2006) "Gibraltar: A Mobile Host-Based Intrusion Protection System", *Proceedings from the 2006 World Congress in Computer Science, Computer Engineering, and Applied Computing*, Jun 26-29, 2006.

Jacoby, G.A., Marchany, R and Davis, N.J. IV (2004) "Battery-based intrusion detection a first line of defense", *Proceedings from the Fifth Annual IEEE SMC, Information Assurance Workshop*, 2004, pp 272-279, ISBN: 0-7803-8572-1

Kannadiga, P., Zulkernine, M. and Ahamed, S.I. (2005) "Towards an Intrusion Detection System for Pervasive Computing Environments", *Proceedings of the International Conference on information technology: coding and Computing (ITCC'05)*, pp 277- 282, Vol. 2, ISBN: 0-7695-2315-3

Martin, T., Hsiao, M., Ha, D. and Krishnaswami, J. (2004) "Denialof- Service Attacks on Battery-powered Mobile Computers", *Second IEEE International Conference on Pervasive Computing and Communications*, pp. 309-318

McAfee (2007) "McAfee, Inc. Reports Preliminary First Quarter Revenue of $314 million", available at: http://www.mcafee.com/us/about/press/corporate/2007/20070426_181010_l.html, date accessed: 16 September 2008

Metropolitan Police Service (2008) "Safeguarding your mobile phone", available at: http://www.met.police.uk/crimeprevention/phone.htm, date accessed: 26 August 2008

MIT (2008) "MIT Media Lab: Reality Mining" available at: http://reality.media.mit.edu/ date accessed: 10 September 2008

Moreau, Y., Verrelst, H., amd Vandewalle, J. (1997) "Detection of mobile phone fraud using supervised neural networks: A first prototype", *International Conference on Artificial Neural Networks Proceedings (ICANN'97)*, pages 1065--1070, October 1997

Muir, J (2003) "Decoding Mobile Device Security", available at: http://www.computerworld.com/securitytopics/security/story/0,10801,82890,00.html, date accessed: 19 October 2007

Ofcom (2007) "The International Communications Market 2007", research document, available at: http://www.ofcom.org.uk/research/cm/icmr07/icmr07.pdf, date accessed: 09 January 2009

Perelson. S. and Botha, R.A. (2004) “An Investigation into Access Control for Mobile Devices”, *ISSA 2004*, Gallagher Estate, Johannesburg, South Africa

Rao, J.R., Rohatgi, P., Scherzer, H. and Tinguely, S (2002) "Partitioning Attacks: Or How to Rapidly Clone Some GSM Cards", *IEEE Symposium on Security and Privacy*, 2002, sp, p. 31,

Stefan A. (2000) “Intrusion Detection Systems: A Survey and Taxonomy”, Department of Computer Engineering, Chalmers University of Technology, Goteborg, Sweden

Sun, B., Chen, Z., Wang, R., Yu, F and Leung, V.C.M. (2006) “Towards adaptive anomaly detection in cellular mobile networks”, *Consumer Communications and Networking Conference, 2006 (CCNC 2006)*, Vol:2, pp. 666-670, ISBN: 1-4244-0085-6

Sun, B., Yu, F., Wu, K. and Leung, VCM (2004) “Mobility-based anomaly detection in cellular mobile networks”, *Proceedings of ACM wireless security (WiSe’ 04)*, Philadelphia, PA, 2004, pp. 61-69

Swami, Y. P. and Tschofenig, H (2006) “Protecting mobile devices from TCP flooding attacks”, *Proceedings of first ACM/IEEE international workshop on Mobility in the evolving internet architecture*, pp. 63 – 68, 2006